TUGAS AKHIR - TE 141599

PENINGKATAN KEAMANAN ADS-B DENGAN ALGORITMA BLOWFISH

Renato Simon Lawalata
NRP 2213100032

Pembimbing
Dr. Ir. Endroyono, DEA.

DEPARTEMEN TEKNIK ELEKTRO
Fakultas Teknologi Elektro
Institut Teknologi Sepuluh Nopember
Surabaya 2017

Halaman ini sengaja dikosongkan

FINAL PROJECT – **TE 141599**

ADS-B SECURITY IMPROVEMENT WITH BLOWFISH ALGORITHM

Renato Simon Lawalata
NRP 2213100032

Supervisor
Dr. Ir. Endroyono, DEA.

DEPARTMENT OF ELECTRICAL ENGINEERING
Faculty of Electrical Technology
Institut Teknologi Sepuluh Nopember
Surabaya 2017

Halaman ini sengaja dikosongkan

PERNYATAAN KEASLIAN
TUGAS AKHIR

Dengan ini saya menyatakan bahwa isi sebagian maupun keseluruhan Tugas Akhir saya dengan judul **"Peningkatan Keamanan ADS-B dengan Algoritma Blowfish"** adalah benar-benar hasil karya intelektual mandiri, diselesaikan tanpa menggunakan bahan-bahan yang tidak diijinkan dan bukan merupakan karya pihak lain yang saya akui sebagai karya sendiri.

Semua referensi yang dikutip maupun dirujuk telah ditulis secara lengkap pada daftar pustaka.

Apabila ternyata pernyataan ini tidak benar, saya bersedia menerima sanksi sesuai peraturan yang berlaku.

Surabaya, 24 Juli 2017

Renato Simon Lawalata
Nrp 2213 100 032

Halaman ini sengaja dikosongkan

PENINGKATAN KEAMANAN ADS-B DENGAN ALGORITMA BLOWFISH

TUGAS AKHIR

Diajukan Guna Memenuhi Sebagian Persyaratan Untuk
Memperoleh Gelar Sarjana Teknik Elektro
Pada
Bidang Studi Telekomunikasi Multimedia
Departemen Teknik Elektro
Institut Teknologi Sepuluh Nopember

Menyetujui

Dosen Pembimbing,

Dr. Ir. Endroyono, DEA
NIP. 196504041991021001

SURABAYA
JULI, 2017

Halaman ini sengaja dikosongkan

Peningkatan Keamanan ADS-B Dengan Algoritma Blowfish

Nama : Renato Simon Lawalata
Pembimbing : Dr. Ir. Endroyono, DEA

ABSTRAK

Teknologi *Automatic Dependent Surveillance-Broadcast* (ADS-B) merupakan salah satu komponen penting dalam *Air Trafic Management* (ATM) masa depan. ADS-B memungkinkan pelacakan pesawat oleh stasiun darat dengan lebih akurat sehingga potensi pesawat keluar jalur atau bahkan hilang dapat diminimalisir.

Salah satu kelemahan dari teknologi ADS-B adalah keamanan kanal transmisi antara pesawat dengan stasiun darat yang lemah sehingga siapapun dengan *receiver* ADS-B dapat menerima sinyal yang dipancarkan pesawat, termasuk berbagai informasi dengan tingkat kerahasiaan tinggi seperti informasi militer. Untuk itu, diperlukan teknik enkripsi data yang baik untuk menyulitkan *receiver* ADS-B yang tidak resmi memperoleh informasi tersebut. Teknik yang digunakan adalah Algoritma Blowfish, algoritma enkripsi simetris dengan kecepatan enkripsi dan dekripsi tinggi dan *throughput* besar. Kekuatan enkripsi akan diukur melalui perhitungan *Avalanche Effect* dan koefisien korelasi antara data asli dengan data hasil enkripsi. Melalui teknik ini diharapkan keamanan data baik dan proses dekripsi tidak memakan banyak waktu, sehingga performansi keseluruhan sistem ADS-B meningkat.

Hasil simulasi menunjukkan bahwa algoritma enkripsi yang disimulasikan dapat bekerja sesuai rencana dengan nilai Avalanche Effect lebih dari atau sama dengan 50% didapat di *round* 10 dan 16, rata-rata koefisien korelasi senilai -0,004716, dan dibutuhkan waktu selama $4{,}175017 \times 10^{15}$ detik untuk dibongkar menggunakan *brute force attack*. Algoritma enkripsi tersebut menghasilkan tambahan waktu pemrosesan infromasi di *receiver* selama rata-rata 94,4 milidetik. Sebagai tambahan simulasi kanal menunjukkan bahwa untuk mendapatkan BER tertentu, SNR kanal Rayleigh harus lebih tinggi dibanding SNR kanal AWGN.

Kata Kunci: ADS-B, *security*, Blowfish

Halaman ini sengaja dikosongkan

ADS-B Security Improvement with Blowfish Algorithm

Name : Renato Simon Lawalata
Advisor : Dr. Ir. Endroyono, DEA

ABSTRACT

Automatic Dependent Surveillance-Broadcast (ADS-B) is one of the *key* components of future *Air Traffic Management* (ATM). ADS-B allows ground station to track airplanes more accurately to minimize the potency of airplanes being out of course and even lost.

One of the concerning aspect of ADS-B technology is the loose security of the transmission channel between the airplane and the ground station so that anyone with an ADS-B signal receiver could receive the signal transmitted from airplanes, which might include highly classified information such as military information. Therefore, it is necessary to add a strong encryption algorithm to make it harder for unlicensed ADS-B signal receivers to obtain the information. The algorithm simulated is Blowfish Algorithm, a symmetric encryption algorithm with high-speed encryption and decryption process and large throughput. The strength of the encryption is measured from the *Avalanche Effect* and correlation coefficient between the real data and the encrypted data. With this algorithm, it is expected that the ADS-B transmission system will have a better security without a time-consuming decryption process, thus increasing the overall performance of ADS-B.

Simulation results show that the encryption algorithm works as planned with Avalanche Effect greater than or equal to 50% obtained in round 10 and 16, average correlation coefficient -0.004716, and it takes $4{,}175017 \times 10^{15}$ seconds to break the algorithm with brute force attack. The encryption algorithm adds an average of 94,4 miliseconds to the data processing duration in the receiver. In addition, channel simulation shows that to obtain a certain value of BER, the SNR of Rayleigh Channel must be higher than the SNR of AWGN Channel.

Keywords: ADS-B, security, Blowfish

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Dengan mengucap puji syukur kepada Tuhan Yang Maha Esa atas limpahan rahmat dan berkat-Nya, sehingga penulis dapat menyelesaikan buku Tugas Akhir ini dengan judul:

PENINGKATAN KEAMANAN ADS-B DENGAN ALGORITMA BLOWFISH

Tugas Akhir ini disusun sebagai salah satu persyaratan dalam menyelesaikan studi pada bidang studi Telekomunikasi Multimedia di jurusan Teknik Elektro, Institut Teknologi Sepuluh Nopember Surabaya.

Dalam kesempatan ini, penulis ingin menyampaikan rasa terima kasih kepada pihak-pihak yang telah mendukung penulis selama proses menyelesaikan Tugas Akhir ini, khususnya kepada:

1. Tuhan Yang Maha Esa atas berkat, rahmat, dan tuntunanNya bagi penulis dari dulu, sekarang saat pengerjaan Tugas Akhir ini, dan sampai seterusnya
2. Kedua orangtua tercinta, Bapak Floyd Wilbert Ray Lawalata dan Ibu Eti Mandiangan, dan kakak sekaligus sahabat, Rafael Stefan Lawalata, yang terus memberikan dukungan bagi penulis khususnya dukungan finansial dan moral selama penulis melaksanakan perkuliahan tingkat sarjana di ITS
3. Bapak Dr. Ir. Endroyono, DEA selaku dosen pembimbing, atas segala ilmu yang diajarkan dan bimbingan yang diberikan, khususnya selama proses pengerjaan Tugas Akhir ini
4. Teman-teman anggota Lab. Komunikasi Multimedia (B304) khususnya sesama pejuang Tugas Akhir yaitu Kevin, Faza, Dzakwan, Feris, David Pui yang jarang muncul, hingga Hilmy atas segala pembelajaran, saran, dan pertemanan yang diberikan
5. Teman-teman dan dosen-dosen bidang studi Telekomunikasi Multimedia, mulai dari Lab. Jaringan Telekomunikasi hingga Lab. Antena dan Propagasi, S1 dan Lintas Jalur, atas segala pertemanan dan bimbingan kepada penulis selama proses perkuliahan hingga pengerjaan Tugas Akhir ini
6. Segenap keluarga e53 yang unpredictable, sebagai sahabat dan keluarga saya di Surabaya serta teman seperjuangan meraih ilmu dan gelar sarjana di Departemen Teknik Elektro selama 4 tahun ini

7. Adik-adik e54 anggota bidang studi Telekomunikasi Multimedia, sebagai sahabat yang ikut mengingatkan penulis untuk fokus pada kegiatan perkuliahan, pengembangan diri, hingga pengerjaan Tugas Akhir ini

Dalam penyusunan laporan Tugas Akhir ini penulis menyadari adanya keterbatasan. Oleh karena itu penulis sangat terbuka terhadap kritik dan saran untuk perbaikan karya Tugas Akhir ini.

Semoga buku Tugas Akhir ini dapat memberikan informasi dan manfaat bagi pembaca pada umumnya dan mahasiswa Departemen Teknik Elektro bidang Studi Telekomunikasi Multimedia pada khususnya. Dan lebih jauh diharapkan mampu memberi kontribusi terhadap perkembangan keilmuan, khususnya di bidang telekomunikasi.

Surabaya, Juli 2017

Penulis

DAFTAR ISI

Halaman ini sengaja dikosongkan

TABLE OF CONTENTS

Halaman ini sengaja dikosongkan

DAFTAR GAMBAR

DAFTAR TABEL

Halaman ini sengaja dikosongkan

BAB 1
PENDAHULUAN

1.1 Latar belakang

Teknologi pelacakan pesawat saat ini mengandalkan RADAR di darat dan komunikasi radio antar pesawat. Kedua teknologi ini sudah terjamin performanya dan telah digunakan untuk waktu yang lama. Terdapat teknologi tambahan yang menjanjikan untuk menjadi kunci dari teknologi *Air Traffic Management* (ATM) masa depan, yaitu *Automatic Dependent Surveillance – Broadcast* (ADS-B).

Dengan ADS-B, pelacakan pesawat menjadi lebih mudah karena sensor-sensor ADS-B yang ukurannya relatif lebih kecil dari antenna RADAR bisa dipasang dimana saja dan oleh siapa saja, tidak terbatas area seperti RADAR di darat yang hanya bisa diletakkan di fasilitas tertentu milik instansi tertentu. ADS-B mengirimkan data-data penerbangan yang sangat penting dalam deteksi keberadaan pesawat seperti *call sign* pesawat, ketinggian, dan *heading*.

Namun karena kemudahan memasang sensor ADS-B tersebut, keamanan ADS-B dianggap masih mungkin bermasalah karena siapa saja bisa menerima dan mengolah data yang diterima, sehingga menjadi potensi masalah jika data yang diterima adalah dari pesawat dengan informasi rahasia seperti informasi militer atau misi khusus lain. Untuk itu, keamanan ADS-B harus ditingkatkan.

1.2 Rumusan Masalah

Permasalahan yang dibahas dalam Tugas Akhir ini adalah sebagai berikut.

1. Bagaimana keberhasilan kinerja enkripsi/dekripsi dari algoritma enkripsi yang disimulasikan?
2. Berapa nilai Avalanche Effect algoritma enkripsi yang disimulasikan?
3. Berapa nilai koefisien korelasi algoritma enkripsi yang disimulasikan?
4. Bagaimana kekuatan algoritma enkripsi yang disimulasikan terhadap serangan?
5. Berapa tambahan waktu untuk pemrosesan informasi di receiver akibat penambahan algoritma enkripsi?

6. Bagaimana pengaruh jenis kanal dan perubahan nilai SNR terhadap BER sistem?

1.3 Batasan Masalah

Pengerjaan Tugas Akhir ini dibatasi pada hal-hal sebagai berikut:

1. Sistem uji adalah ADS-B dengan format *frame Mode S Reply Extended Squitter downlink* (dari pesawat ke stasiun darat)
2. Algoritma enkripsi yang digunakan adalah Algoritma Blowfish dengan ukuran blok sebesar 8 bit, tanpa membahas proses distribusi *key*
3. Simulasi sistem dilakukan dengan *software* MATLAB R2016a
4. Kanal transmisi yang disimulasikan adalah kanal AWGN dan kanal Rayleigh
5. Komputer yang digunakan untuk melakukan simulasi adalah laptop dengan prosesor Intel Core i5-5200U dengan *clock speed* 2,2 GHz dan RAM 4 GB

1.4 Tujuan

Tujuan dari penulisan Tugas Akhir ini adalah sebagai berikut.

1. Menerapkan algoritma enkripsi pada simulasi sistem ADS-B dan memberikan analisa terhadap performa algoritma enkripsi yang diterapkan pada sistem dan performa sistem secara keseluruhan setelah penambahan algoritma enkripsi
2. Memberikan analisa performa sistem ADS-B yang telah dimodifikasi di 2 macam kanal transmisi, yaitu kanal AWGN dan kanal Rayleigh

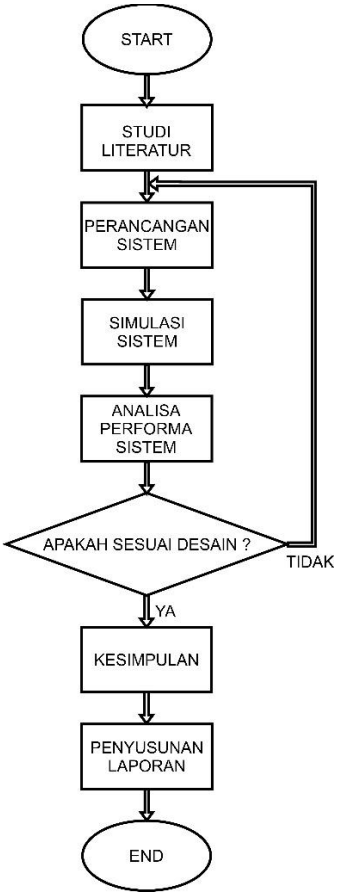
1.5 Metodologi

Pengerjaan Tugas Akhir ini dilakukan melalui beberapa tahapan yaitu studi literatur, perancangan sistem, simulasi sistem hasil rancangan, analisa performa sistem dari hasil simulasi, pembuatan kesimpulan dan penyusunan laporan Tugas Akhir, sebagaimana ditunjukkan dalam Gambar 1.1 berikut.

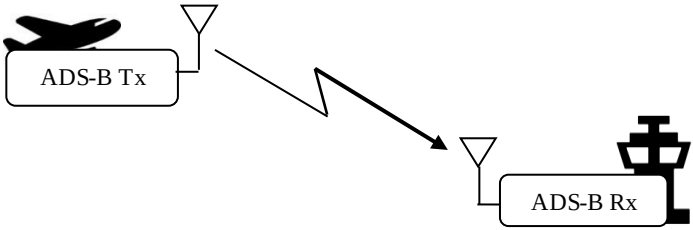
Studi literatur dilakukan untuk mendasarkan penelitian pada bahan-bahan literatur dan jurnal-jurnal penelitian yang telah dilakukan pada penelitian sebelumnya mengenai keamanan ADS-B dan Algoritma Blowfish. Selanjutnya akan dilakukan perancangan sistem sesuai kebutuhan desain yang diinginkan. Berikut ilustrasi sistem ADS-B,

dengan siaran ADS-B dari pesawat ke stasiun darat, yang menjadi acuan dalam pengerjaan Tugas Akhir.

Simulasi sistem dilakukan dengan menggunakan variabel-variabel sesuai rancangan yang telah dibuat. Melalui tahap ini diharapkan terbentuk sistem rancangan yaitu adanya penambahan algoritma enkripsi yang terintegrasi dengan sistem yang saat ini ada. Simulasi sistem dilakukan dengan MATLAB dan simulasi menggunakan pendekatan simulasi *baseband* dari ADS-B.



Gambar 1.1 *Flowchart* Metodologi Tugas Akhir



Gambar 1.2 Ilustrasi Sistem ADS-B dari Pesawat ke Stasiun Darat

Informasi yang disimulasikan berasal dari *frame generator* ADS-B. Format data yang digunakan adalah ADS-B *Mode S Extended Squitter*, yang terdiri dari 112 bit data. Sistem enkripsi dan dekripsi yang disimulasikan sesuai dengan metode yang diusulkan, yaitu Algoritma Blowfish dengan ukuran blok 8 bit. Modulasi yang digunakan adalah modulasi PPM (*Pulse Position Modulation*). Output dari sistem adalah bit-bit estimasi informasi ADS-B yang melewati suatu *frame detector*.

Selanjutnya dilakukan analisa terhadap performa algoritma enkripsi rancangan berdasarkan hasil simulasi. Jika ditemukan kesalahan atau ketidaksesuaian dengan desain, maka diadakan perbaikan terhadap algoritma enkripsi rancangan hingga hasil simulasi menunjukkan algoritma telah bekerja sesuai desain.

Keamanan skema enkripsi yang diusulkan diukur melalui perhitungan *Avalanche Effect* dan koefisien korelasi. Selain itu, diberikan analisa keamanan skema enkripsi terhadap serangan berupa *brute force attack*. Kecepatan persiapan proses enkripsi dan kecepatan proses dekripsi diukur untuk memberikan gambaran mengenai performa sistem ADS-B setelah penambahan algoritma enkripsi.

Setelah simulasi bekerja sesuai desain, berbagai data dapat diambil untuk kemudian dianalisa. Kesimpulan dari percobaan dapat disusun berdasarkan analisa terhadap berbagai data yang didapat dalam simulasi.

Tahapan akhir adalah penyusunan laporan Tugas Akhir berdasarkan simulasi yang telah dilakukan dan hasil yang didapat dari simulasi sesuai dengan kaidah penulisan Tugas Akhir.

1.6 Sistematika Penulisan

Tugas Akhir ini dibagi menjadi 5 bab dengan sistematika sebagai berikut.

BAB I Pendahuluan

Bab ini meliputi latar belakang, permasalahan, tujuan penelitian, metodologi penelitian, sistematika penulisan, dan relevansi Tugas Akhir.

BAB II Teori Penunjang

Bab ini berisi teori-teori dasar tentang sistem ADS-B, teori dasar kriptografi, termasuk didalamnya teori dasar Algoritma Blowfish sebagai algoritma yang akan diterapkan, teori mengenai parameter pengukuran keamanan informasi, dan teori dasar kanal transmisi yang akan disimulasikan.

BAB III Pemodelan Simulasi

Bab ini berisi desain simulasi yang akan dilakukan yang terdiri dari desain sistem ADS-B keseluruhan, mulai dari pembangkitan *frame* ADS-B, pengolahan informasi di *transmitter*, kanal transmisi, hingga pengolahan informasi di *receiver*, desain Algoritma Blowfish 8 bit, dan skenario-skenario pengambilan data hasil simulasi yaitu pengukuran performa algoritma enkripsi, pengukuran performa sistem di kanal transmisi, dan pengukuran parameter keamanan informasi.

BAB IV Analisa Hasil Simulasi

Bab ini berisi analisa terhadap data hasil simulasi yang diperoleh dari berbagai skenario pengukuran yang dijelaskan di BAB III, yaitu mulai dari analisa performa algoritma enkripsi, analisa performa sistem di kanal transmisi, dan analisa berbagai parameter keamanan informasi.

BAB V Penutup

Bab ini berisi kesimpulan yang disesuaikan dengan hasil analisa di BAB IV dan saran bagi penelitian selanjutnya.

1.7 Relevansi / Manfaat

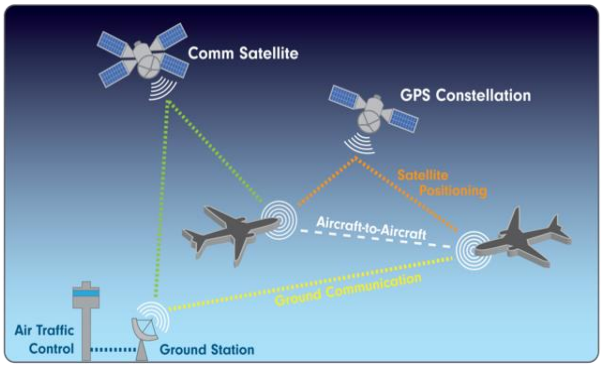
Hasil dari Tugas Akhir ini adalah analisa terhadap suatu sistem rancangan berupa sistem ADS-B dengan penambahan algoritma enkripsi yang memungkinkan peningkatan keamanan data-data yang disiarkan dalam sistem ADS-B, dengan harapan hanya pihak yang memiliki otoritas yang dapat memperoleh informasi ADS-B, sebagai bentuk dukungan terhadap *Air Traffic Management* (ATM) masa depan.

Halaman ini sengaja dikosongkan

BAB 2
TEORI PENUNJANG

2.1 Automatic Dependent Surveillance – Broadcast (ADS-B)

ADS-B, sesuai [1] dan [2], adalah salah satu teknologi di bidang *broadcasting* yang menjadi kunci *Air Traffic Management* (ATM) masa depan. ADS-B mendukung kemampuan pembaharuan informasi pesawat dengan lebih cepat dan dengan akurasi lebih tinggi dari teknologi RADAR, ditambah dengan kemampuan perluasan daerah *Air Traffic Control* (ATC) ke daerah yang belum terjangkau oleh RADAR. ADS-B adalah teknologi yang memungkinkan pesawat mengirimkan informasi penerbangan seperti posisi, ketinggian, dan kecepatan secara otomatis.

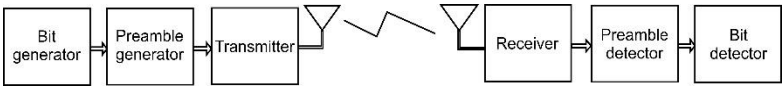


Gambar 2.1 Ilustrasi Sistem ADS-B

Sistem ADS-B terdiri dari perangkat di pesawat, kanal transmisi, dan stasiun darat, seperti yang ditunjukkan Gambar 2.1 [3]. Perangkat di pesawat akan menghimpun informasi-informasi yang berguna dalam sistem navigasi pesawat dan menyiarkannya untuk diterima oleh stasiun darat sehingga bisa digunakan untuk keperluan ATC sebagai pendukung RADAR, dan oleh pesawat-pesawat lain disekitarnya untuk bantuan navigasi. Dengan bantuan informasi ADS-B, pilot dapat melihat pesawat-pesawat lain yang ada disekitarnya secara *real-time* (transmisi ADS-B dilakukan tiap detik) melalui *display* [4] sehingga tingkat kewaspadaan pilot dapat meningkat karena tidak hanya mengandalkan faktor penglihatan pilot ke ruang udara di depannya dan informasi yang didapat dari stasiun darat.

Gambar 2.2 *Display* ADS-B

Perangkat di pesawat memiliki kemampuan mengirim dan menerima informasi melalui ADS-B. Transmisi informasi ADS-B yang keluar dari suatu pesawat disebut *ADS-B Out*. Penerimaan informasi ADS-B oleh suatu pesawat disebut *ADS-B In*. Sistem *ADS-B Out* lebih diprioritaskan untuk dipasang dibanding *ADS-B In* karena mendukung teknologi RADAR dalam deteksi keberadaan pesawat di ruang udara yang ada; tanpa *ADS-B In*, pendeteksian pesawat tetap bekerja.

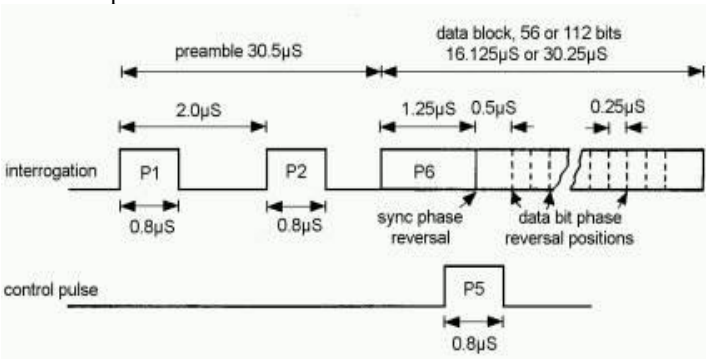


Gambar 2.3 Blok Diagram RF ADS-B

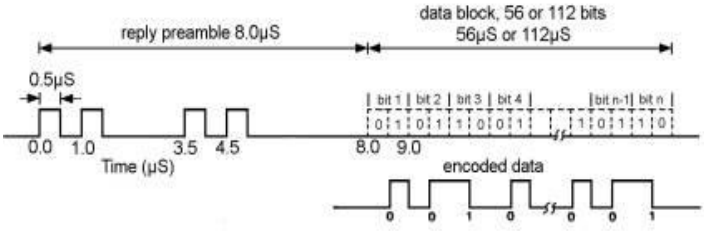
Walaupun ADS-B telah disertifikasi dan digunakan di industri untuk waktu yang lama, keamanan ADS-B masih menjadi topik hangat untuk diteliti terutama di sisi autentikasi, kerahasiaan, integritas, dan ketersediaan pesan ADS-B. Penelitian sebelumnya [5] menyatakan bahwa pesan ADS-B rentan terhadap beberapa serangan, diantaranya *eavesdropping*, *jamming*, *message injection*, *message deletion*, dan *message modification*. Penelitian ini telah mencoba menyelesaikan

masalah ini dengan mengembangkan suatu sistem enkripsi simetris bertahap.

ADS-B menggunakan transponder dengan format pulsa *Mode S* yang diterapkan dalam sistem RADAR. Secara umum, sinyal *Mode S* terbagi menjadi 2, yaitu *Mode S Interrogation* dan *Mode S Reply*, masing-masing berfungsi untuk menanyakan informasi mengenai pesawat yang berada di jangkauan siaran dan untuk membalas pertanyaan yang diterima. *Mode S Interrogation* menggunakan modulasi DPSK (*Differential Phase Shift Keying*) dengan *data rate* 4 Mbps. *Mode S Reply* menggunakan modulasi PPM (*Pulse Position Modulation*) dengan *data rate* 1 Mbps.



Gambar 2.4 Format *Mode S Interrogation*



Gambar 2.5 Format *Mode S Reply*

Dalam *Mode S Reply* untuk RADAR, format *frame* data yang digunakan disebut sebagai *Short Squitter* yang terdiri dari 56 bit. ADS-B mengadopsi *Mode S Reply* dalam hal modulasi dan *data rate*, namun

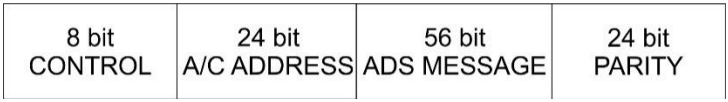
mengembangkan format *frame* datanya dengan menambahkan informasi ADS-B kedalamnya sehingga disebut sebagai *Extended Squitter* yang terdiri dari 112 bit.

Gambar 2.6 Format *Frame Mode S* Short *Squitter*

Perangkat ADS-B bekerja dalam 2 frekuensi, 1090 MHz dan 978 MHz. Karena bekerja di 2 frekuensi berbeda, di stasiun darat ADS-B terdapat proses penerjemahan, format ulang, dan penyiaran ulang informasi dari tiap frekuensi sehingga semua pesawat dapat menerima dan mengolah semua informasi dari tiap-tiap pesawat.

2.1.1 *Extended Squitter*

Mode *Extended Squitter* adalah mode ADS-B yang menggunakan frekuensi 1090 MHz sebagai *center frequency* sinyal pembawanya. Mode ini disingkat namanya menjadi 1090ES. 1090ES bekerja berdasarkan format ADS-B *Mode S* dan lebih banyak digunakan di pesawat komersial. Ukuran tipikal *payload* 1090ES adalah 56 bit, diantaranya 5 bit untuk *Downlink Format* (DF) untuk menjelaskan tipe pesan, 3 bit *Capability* (CA) untuk indikator kemampuan transponder *Mode S* atau subtipenya, 24 bit *ICAO Address* (disebut juga nomor ekor pesawat), dan 24 bit *Parity Information* (PI).



Gambar 2.7 Format *Frame Mode S Extended Squitter*

Menurut referensi [6], 56 bit pesan ADS-B terdiri dari beberapa bagian, secara berurutan yaitu: 5 bit *Type Code* (berisi informasi mengenai jenis informasi yang ada di bit ke 9 hingga bit ke 56), 3 bit *Emmiter Category* (berisi informasi jenis emitter yang digunakan), dan 48 bit informasi (6 karakter, masing-masing tersusun dari 8 bit).

2.1.2 *Universal Access Transceiver*

Universal Access Transceiver [7] adalah mode ADS-B yang menggunakan frekuensi 978 MHz sebagai *center frequency* sinyal pembawanya. Ukuran tipikal *payload* ADS-B dalam UAT adalah 272 bit dengan format framenya diawali dengan 36 bit untuk sinkronisasi (SYNC) dan diakhiri dengan 112 bit untuk *forward error correction parity information* (FEC PARITY).

Gambar 2.8 Format *Frame Universal Access Transceiver*

2.2 Kriptografi

Kriptografi [8] merujuk kepada usaha yang dilakukan untuk merahasiakan informasi yang akan ditransmisikan sebagaimana hingga informasi tersebut hanya dipahami oleh pihak pengirim dan penerima tertentu. Informasi diacak menggunakan suatu kunci dan dapat dikembalikan seperti semula menggunakan suatu kunci. Proses penguncian informasi sebelum transmisi disebut enkripsi sementara dekripsi merujuk pada usaha untuk membuka kunci dari informasi yang telah melalui proses enkripsi sehingga informasi asli menjadi terbuka dan dapat diolah lebih lanjut.

Dalam kriptografi, informasi asli disebut sebagai *plaintext* dan informasi hasil pengacakan disebut ciphertext atau *cipher*. Suatu *cipher* dikatakan baik apabila memiliki kemungkinan kecil untuk dapat dikembalikan menjadi *plaintext* dalam waktu yang singkat. Dalam kriptografi modern, algoritma kriptografi tidak dirahasiakan; semua orang dapat mengetahui bagaimana cara kerja suatu algoritma kriptografi. Kunci untuk melakukan enkripsi dan dekripsilah yang dirahasiakan sehingga pengolahan data hanya dapat dilakukan oleh pihak-pihak tertentu yang mengetahui kunci tersebut. Tingkat kesulitan bagi pihak yang tidak memiliki otoritas atas informasi tersebut untuk menentukan kunci yang tepat adalah suatu ukuran bagi kekuatan pengacakan informasi oleh suatu algoritma enkripsi.

Berdasarkan kunci yang digunakan untuk melakukan enkripsi dan dekripsi, teknik enkripsi dibedakan menjadi 2, yaitu enkripsi simetris dan enkripsi asimetris.

2.2.1 Enkripsi Simetris

Enkripsi simetris adalah teknik enkripsi dimana pihak pengirim dan penerima melakukan proses enkripsi dan dekripsi menggunakan kunci yang sama dan algoritma yang digunakan untuk melakukan enkripsi dan dekripsi adalah sama. Agar pihak pengirim dan penerima informasi memiliki kunci yang sama, diperlukan suatu prosedur khusus untuk mendistribusikan kunci tersebut.

Cara kerja enkripsi simetris, misalkan dalam komunikasi antara pihak A dan B adalah sebagai berikut. Ketika pihak A ingin mengirim informasi yang ingin dienkripsi sebelum dikirim ke pihak B, maka pihak A melakukan enkripsi informasi dengan suatu kunci, dan mendistribusikan kunci tersebut agar diketahui pihak B. Setelah informasi terkirim dan diterima oleh pihak B, maka pihak B bisa melakukan dekripsi dengan kunci yang dimiliki.

Beberapa algoritma enkripsi yang termasuk enkripsi simetris adalah Caesar Cipher, AES (Rijndael), dan Blowfish.

2.2.2 Enkripsi Asimetris

Enkripsi asimetris adalah teknik enkripsi dimana pihak pengirim dan penerima melakukan proses enkripsi dan dekripsi menggunakan kunci yang berbeda, sehingga untuk menyesuaikan dengan perbedaan kunci tersebut, algoritma enkripsi dan dekripsinya menjadi berbeda. Karena pihak pengirim dan penerima tidak menggunakan kunci yang sama, maka teknik ini tidak memerlukan prosedur khusus untuk memastikan kesamaan kunci seperti pada teknik enkripsi simetris.

Cara kerja enkripsi asimetris, misalkan dalam komunikasi antara pihak A dan B adalah sebagai berikut. Ketika pihak A ingin mengirim informasi yang ingin dienkripsi sebelum dikirim ke pihak B, maka pihak A harus melakukan enkripsi informasi dengan kunci publik milik pihak B, yang secara legal dapat diketahui oleh semua pihak. Setelah informasi terenkripsi diterima pihak B, maka pihak B dapat melakukan dekripsi menggunakan kunci privat yang hanya diketahui oleh pihak B. Proses sebaliknya berlaku ketika pihak B ingin mengirim informasi terenkripsi ke pihak A.

Contoh algoritma enkripsi yang termasuk enkripsi asimetris adalah Algoritma Diffie-Hellman, RSA, dan ECC.

2.2.3 *Cryptanalysis*

Cryptanalysis mengacu kepada usaha-usaha untuk menemukan kunci enkripsi dari suatu proses enkripsi. *Cryptanalysis* dapat dilakukan oleh siapa saja yang kompeten di bidang kriptografi (pelaku disebut sebagai *cryptanalist*), dan terhadap algoritma apa saja. Tujuan mulia dari *cryptanalysis* adalah untuk memberikan evaluasi terhadap performa suatu algoritma enkripsi sehingga sang pembuat algoritma dapat meningkatkan performa algoritmanya dan calon pengguna mendapatkan gambaran mengenai kekuatan dari algoritma yang akan dipakai.

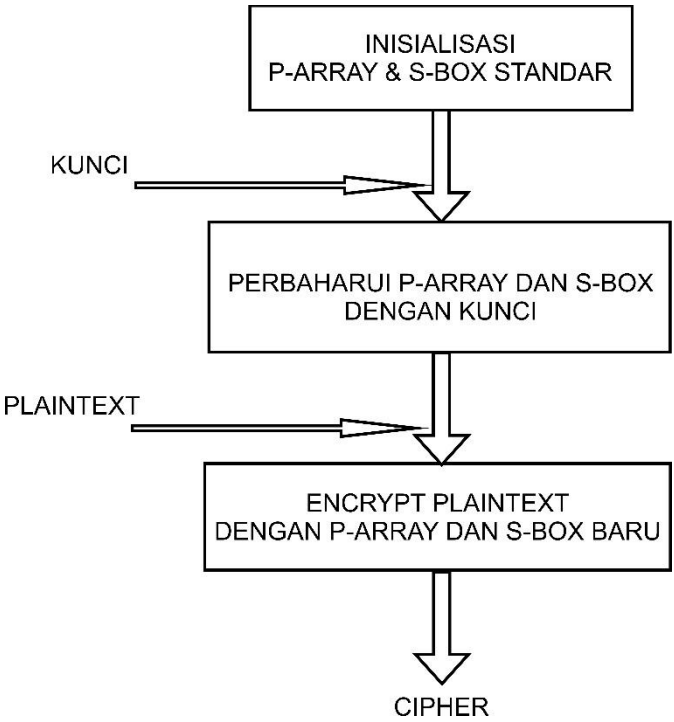
Dalam menguji kekuatan algoritma kriptografi, seorang *cryptanalist* mencoba memperoleh informasi asli dari suatu data hasil enkripsi dengan segala cara, termasuk diantara dengan mencoba-coba berbagai kunci yang dimilikinya untuk membuka kunci enkripsi tersebut. Cara yang dapat dilakukan untuk mendapatkan kunci enkripsi adalah *brute force attack*.

Brute force attack [9] adalah suatu jenis serangan terhadap informasi yang telah dikunci dengan suatu algoritma enkripsi dengan mencoba membuka paksa kuncinya dengan mencoba segala kemungkinan kunci. *Brute force attack* membutuhkan waktu komputasi yang lama karena semua kemungkinan kunci dicoba satu persatu. Akibat cost yang besar inilah, maka suatu algoritma enkripsi dikatakan baik apabila dapat memaksa seorang *cryptanalist* untuk melakukan *brute force attack* untuk mencari kunci enkripsi. Salah satu cara untuk mengukur kecepatan proses *cryptanalysis* adalah menggunakan rumus sebagai berikut.

$$Durasi\ (detik) = Jumlah\ key \times Waktu\ komputasi\ per\ key\ (detik) \quad (2.1)$$

2.3 Algoritma Blowfish

Blowfish [10,11] didasarkan pada *Feistel Network* dengan pengulangan sebanyak 16 kali. Blowfish menggunakan ukuran blok standar 64 bit dan panjang kunci bervariasi dengan maksimal 448 bit. Blowfish cocok diimplementasikan di sistem dimana kunci enkripsi jarang diganti dikarenakan proses inisialisasi kunci enkripsinya memakan waktu yang cukup lama. Blowfish menggunakan *subkey* dalam jumlah banyak dan sebuah *substitution box* yang harus didefinisikan terlebih dahulu sebelum proses enkripsi dan dekripsi.



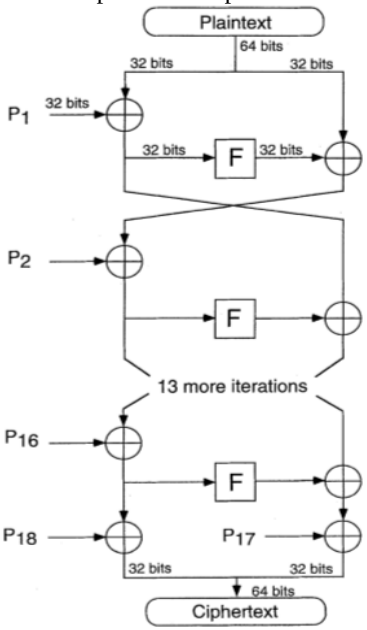
Gambar 2.9 Diagram Blok Cara Kerja Algoritma Blowfish

Beberapa poin spesifikasi Blowfish 64 bit adalah sebagai berikut.

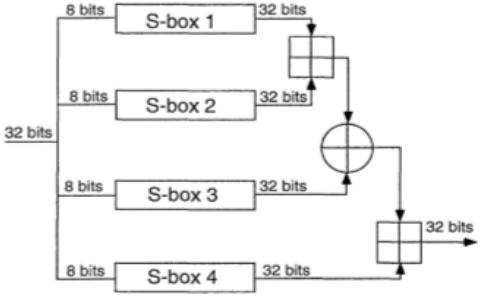
1. P-array terdiri atas 18 *subkey* berukuran 32 bit:
   P1 , P2 , ... , P18

2. Terdapat 4 kotak-S berukuran 32 bit dengan isi masing-masing 256 entri:
   S1,0 , S1,1 , ... , S1,255 ;
   S2,0 , S2,1 , ... , S2,255 ;
   S3,0 , S3,1 , ... , S3,255 ;
   S4,0 , S4,1 , ... , S4,255 ;

Berikut adalah *pseudocode* proses enkripsi dalam Blowfish 64 bit:



Gambar 2.10 DIagram Blowfish 64 Bit



Gambar 2.11 Diagram Blok Fungsi F (*Feistel Network*) Blowfish 64 Bit

Proses dekripsi menggunakan tahapan yang sama, dengan urutan P1 hingga P18 dibalik.

2.4 Parameter Keamanan Informasi

Keamanan suatu informasi dapat dinyatakan dalam nilai kuantitatif dari variabel-variabel tertentu. Variabel tersebut adalah parameter keamanan informasi. Keamanan suatu informasi berkaitan erat dengan performa algoritma enkripsi yang digunakan untuk mengamankan informasi tersebut. Keamanan informasi dapat diukur dari seberapa besar pengaruh kunci yang dimasukkan terhadap *cipher* yang dihasilkan dan seberapa besar keterkaitan atau korelasi antara *cipher* dengan *plaintext*.

2.4.1 *Avalanche Effect*

Avalanche Effect merupakan suatu sifat dari informasi hasil enkripsi, yaitu berapa persen perubahan bit-bit informasi terenkripsi terhadap perubahan 1 bit dalam kunci enkripsi atau *plaintext*. Secara matematis, *Avalanche Effect* dapat dinyatakan sebagai berikut.

$$\text{Avalanche Effect } (\%) = \frac{\sum \text{ bit informasi yang berubah}}{\sum \text{ bit informasi asli}} \, x \, 100\% \qquad (2.2)$$

Nilai *Avalanche Effect* yang tinggi mengindikasikan adanya fenomena dimana perubahan kecil pada *plaintext* atau kunci enkripsi menyebabkan perubahan besar pada *cipher* atau dengan kata lain tingkat kesulitan untuk menebak kunci enkripsi dalam proses *cryptanalysis* menjadi meningkat. Nilai *Avalanche Effect* yang baik adalah lebih besar dari 0,5 yang menunjukkan adanya perubahan pada minimal 50% dari jumlah bit *cipher* ketika *plaintext* atau kunci enkripsi berubah 1 bit.

2.4.2 Koefisien Korelasi

Koefisien korelasi menyatakan tingkat korelasi linier antara 2 variabel dan dapat bernilai positif atau negatif, antara -1 dan +1. Korelasi positif menunjukkan hubungan dimana ketika nilai suatu variabel naik maka nilai variabel lainnya juga naik sementara korelasi negatif menunjukkan hubungan dimana ketika nilai suatu variabel naik, maka nilai variabel lainnya turun. Nilai koefisien korelasi dapat dikategorikan sebagai berikut.

Tabel 2.1 Kategori Koefisien Korelasi

Nilai Koefisien Korelasi	Indikasi Jenis Korelasi
0	Tidak ada korelasi linier
-1	Ada korelasi linier negatif yang sempurna
+1	Ada korelasi linier positif yang sempurna
Antara -0,3 sampai 0 atau 0 sampai 0,3	Ada korelasi linier (positif atau negatif) yang lemah
Antara -0,7 sampai -0,3 atau 0,3 sampai 0,7	Ada korelasi linier (positif atau negatif) yang sedang
Antara -1 sampai -0,7 atau 0,7 sampai 1	Ada korelasi linier (positif atau negatif) yang kuat

2.5 Kanal Transmisi

Dalam transmisi informasi, suatu sinyal informasi akan melalui kanal transmisi. Kanal transmisi disebut juga sebagai media transmisi. Kanal transmisi dapat merujuk pada bentuk fisik, misalnya ada yang berupa kabel seperti kabel tembaga, kabel *twisted pair*, dan kabel optik, atau udara. Dalam komunikasi nirkabel, kanal transmisi merujuk pada frekuensi pembawa yang digunakan dalam suatu komunikasi, misalnya pada teknologi seluler ada yang disebut dengan kanal GSM 900, dimana 900 (dalam satuan MHz) adalah frekuensi tengah dalam komunikasi antara telepon genggam pengguna jaringan dengan BTS.

Kanal siaran ADS-B, dengan frekuensi pembawa 1090 MHz, merupakan kanal nirkabel (udara) yang masuk ke dalam *band* UHF (*Ultra High Frequency*). Komunikasi dalam kanal UHF berbasis pada *link line-of-sight* dan adanya kemungkinan pemantulan sinyal di tanah atau terhalangnya sinyal oleh objek-objek besar seperti bangunan besar, bukit, dan gunung, yang kemungkinan menyebabkan adanya *multipath* dalam *link* komunikasi yang terbentuk. Efek pembiasan sinyal oleh lapisan ionosfer dan redaman akibat gas-gas di udara tidak ada karena panjang gelombang sinyal lebih besar dari partikel-partikel di udara.

Untuk menguji performa suatu sistem komunikasi pada kanal transmisi tertentu, parameter yang bisa dihitung adalah BER (*Bit Error Rate*), sesuai rumus:

$$Bit\ Error\ Rate = \frac{Jumlah\ Bit\ Error}{Jumlah\ Bit\ Total} \tag{2.3}$$

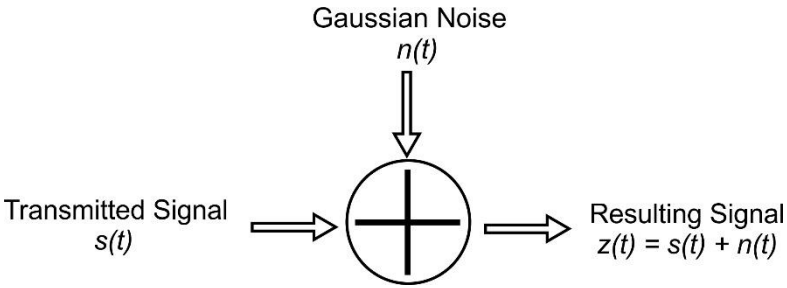
BER menunjukkan berapa banyak jumlah bit yang berbeda dari yang seharusnya atau *error* setelah bit-bit informasi melewati tahap-tahap lebih lanjut dalam sistem komunikasi, seperti proses enkripsi/dekripsi atau saat dilakukan modulasi, dilewatkan ke kanal transmisi, dan demodulasi.

2.5.1 Kanal AWGN

Kanal AWGN (*Additive White Gaussian Noise*) merupakan model kanal transmisi dasar dalam pemodelan sistem komunikasi dan umumnya digunakan untuk pemodelan sistem komunikasi jaringan tetap dengan media transmisi berupa kabel. Sesuai namanya, kanal AWGN memiliki sifat aditif (menambahkan *noise* pada sinyal informasi), memiliki persebaran daya yang sama diseluruh pita frekuensi (layaknya warna putih dalam pita frekuensi cahaya tampak) dan memiliki distribusi normal (Gaussian) dalam domain waktu.

Kanal AWGN merupakan model kanal transmisi dimana antena pengirim dan penerima diasumsikan dalam keadaan diam. Sifat-sifat kanal transmisi seperti *frequency-selective fading*, pemantulan sinyal, dan difraksi sinyal tidak termasuk dalam pemodelan kanal AWGN sehingga tidak terbentuk deskripsi yang lengkap mengenai kanal transmisi dalam dunia nyata namun dapat memberikan gambaran dasar mengenai karakter sistem komunikasi yang diteliti.

Dalam simulasi sistem komunikasi, kanal AWGN mempengaruhi sinyal dengan memberikan atenuasi terhadap amplitudo sinyal dan menambahkan *noise*. Gambar 2.12 memberikan gambaran sederhana mengenai proses yang terjadi di kanal AWGN, dengan sinyal yang ditransmisikan ($s(t)$) akan berubah akibat penambahan *noise* ($n(t)$) menjadi suatu sinyal akhir ($z(t) = s(t) + n(t)$).

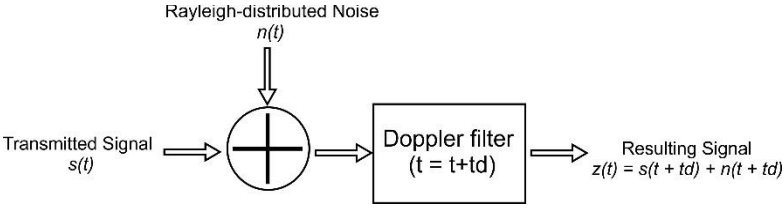


Gambar 2.12 Persamaan Matematis Kanal AWGN

2.5.2 Kanal Rayleigh

Kanal Rayleigh merupakan model kanal transmisi yang digunakan untuk pemodelan sistem komunikasi bergerak, dimana minimal salah satu diantara antena pengirim dan penerima dalam keadaan bergerak. Kanal Rayleigh juga memberikan gambaran mengenai kanal transmisi dalam sistem komunikasi dimana terdapat *obstacle* antara pengirim dan penerima sehingga dapat terjadi pemantulan sinyal, difraksi sinyal, sambil memperhitungkan adanya Efek Doppler pada frekuensi sinyal akibat pergerakan pengirim dan/atau penerima sehingga memberikan deskripsi yang lebih lengkap mengenai kanal transmisi dalam berbagai aplikasi di dunia nyata seperti komunikasi seluler dan komunikasi antar kendaraan.

Dalam simulasi sistem komunikasi, kanal Rayleigh mempengaruhi sinyal informasi dengan memberikan atenuasi terhadap amplitudo sinyal, memberikan Efek Doppler, dan menambahkan *noise*. Gambar 2.13 memberikan gambaran sederhana mengenai proses yang terjadi pada kanal Rayleigh dimana sinyal yang ditransmisikan ($s(t)$) akan mengalami penambahan *noise* ($n(t)$) menjadi suatu sinyal ($s(t) + n(t)$), dan sinyal tersebut mengalami Efek Doppler, yaitu pergeseran dalam domain waktu sebesar satuan waktu tertentu (td), dapat dituliskan sebagai ($z(t) = s(t+td) + n(t+td)$).



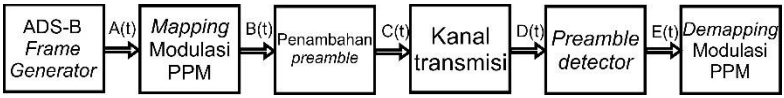
Gambar 2.13 Persamaan Matematis Kanal Rayleigh

Halaman ini sengaja dikosongkan

BAB 3
PEMODELAN SIMULASI

3.1 Pemodelan *Baseband* ADS-B

Sistem ADS-B disimulasikan menurut model simulasi *baseband* dan terdiri dari bagian *transmitter* ADS-B yang didalamnya terdiri dari *bit stream generator* dan bagian *mapping* modulasi PPM serta bagian *receiver* ADS-B yang didalamnya terdiri dari bagian pengenal *preamble* dan bagian *demapping* modulasi PPM. Diagram blok sistem adalah sebagai berikut.



Gambar 3.1 Model Sistem ADS-B

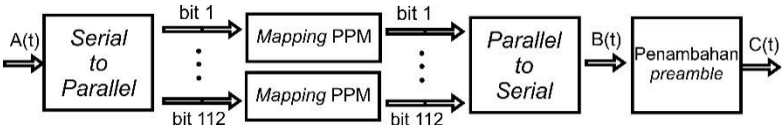
3.1.1 Pembentukan Format *Frame* ADS-B

Informasi ADS-B yang disimulasikan adalah sesuai dengan *Mode S Reply Extended Squitter* yaitu sejumlah 112 bit dan dalam simulasi dinyatakan sebagai 112 bit (nilai 1 atau 0) yang dibangkitkan secara acak, dimana pada Gambar 3.1 ditunjukkan oleh simbol A(t).

3.1.2 Pemodelan *Transmitter* ADS-B

Setelah proses enkripsi 112 bit informasi ADS-B, tahapan selanjutnya adalah penambahan bit-bit *preamble* sebagai tanda pengenal sinyal ADS-B *Mode S Reply* dan melakukan *mapping* bit-bit sesuai modulasi PPM. Dalam simulasi, dilakukan *mapping* sebelum penambahan bit-bit dan *mapping preamble* untuk menyederhanakan proses *mapping preamble* yang bentuk sinyalnya tidak sesuai jika *mapping* dilakukan bersamaan dengan bit-bit informasi.

Skema *transmitter* ADS-B yang disimulasikan adalah sesuai Gambar 3.2 berikut.

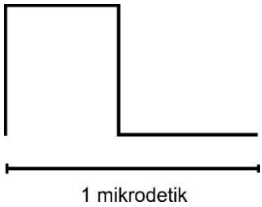


Gambar 3.2 Skema *Transmitter* ADS-B

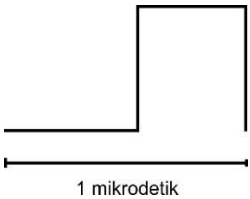
3.1.2.1 *Mapping Modulasi PPM*

Mapping modulasi PPM dilakukan dengan pembentukan sinyal rektangular B(t) dengan *duty cycle* 50% dengan durasi 1 mikrodetik. Untuk setiap bit informasi dilakukan *upsampling* menjadi 10 sampel, sehingga periode per sampel menjadi 0.1 mikrodetik.

Mapping dilakukan sesuai dengan bentuk pulsa PPM yang diterapkan dalam sistem ADS-B seperti pada gambar-gambar berikut.



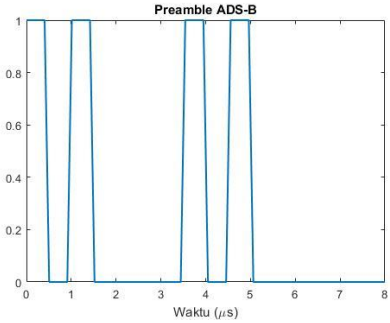
Gambar 3.3 Pulsa PPM Representasi Bit 0



Gambar 3.4 Pulsa PPM Representasi Bit 1

3.1.2.2 *Penambahan Preamble & Pembentukan Sinyal ADS-B*

Preamble sinyal ADS-B adalah seperti di Gambar 3.4.



Gambar 3.5 Format *Preamble* ADS-B

Akibat format yang demikian, maka *preamble* tidak bisa dinyatakan dalam bit-bit terlebih dahulu bersamaan dengan bit-bit informasi sebelum *mapping* bersamaan sehingga *mapping preamble* dilakukan secara terpisah.

Penambahan *preamble* diawali dengan membangkitkan bit-bit *preamble* sejumlah 16 bit. Selanjutnya untuk setiap bit *preamble* dilakukan *upsampling* menjadi 5 sampel untuk membentuk pulsa *preamble* sesuai ketentuan. Sinyal akhir yang terbentuk ditunjukkan oleh simbol C(t) pada Gambar 3.1.

3.1.3 Pemodelan *Receiver* ADS-B

Setelah sinyal informasi ADS-B melalui kanal, sinyal tersebut diterima oleh *receiver* ADS-B. Tahapan pertama yang dilakukan adalah mengenali *preamble* sinyal ADS-B sebagai identitas sinyal ADS-B kemudian melakukan *demapping* pulsa PPM menjadi bit-bit estimasi informasi ADS-B.

3.1.3.1 *Mengenali Preamble*

Tahapan ini dilakukan dengan memisahkan *preamble* sinyal yang sudah diketahui porsinya dalam keseluruhan sinyal yang diterima (simbol D(t) pada Gambar 3.1) dan memastikan apakah sebagian sinyal tersebut adalah *preamble* sinyal informasi ADS-B. Setiap 5 sampel per bit *preamble* akan dicari nilai rata-ratanya dan diputuskan apakah merupakan bit 1 atau bit 0 (*downsampling* dari 5 sampel ke 1 sampel).

3.1.3.2 *Demapping Modulasi PPM*

Setelah *preamble* sinyal informasi ADS-B dipastikan sudah benar, maka selanjutnya sebagian sinyal tempat informasi ADS-B berada (simbol E(t) pada Gambar 3.1) diolah dengan melakukan *downsampling* dari 10 sampel ke 1 sampel. Tiap 10 sampel diambil nilai rata-ratanya dan diputuskan apakah merupakan bit 1 atau bit 0, sehingga membentuk bit-bit estimasi informasi ADS-B.

3.2 Pemodelan Simulasi *Baseband*

Simulasi sistem ADS-B yang dilakukan adalah simulasi *baseband* sesuai Gambar 3.5 pada halaman berikutnya.

Gambar 3.6 Diagram Blok Simulasi *Baseband* ADS-B

Simulasi *baseband* dilakukan untuk menganalisa performa sistem ADS-B yang dirancang pada kanal transmisi, dalam hal ini yaitu kanal AWGN dan kanal Rayleigh. Dalam simulasi, *bit stream generator* menghasilkan bit-bit yang disebut sinyal $x_1(t)$, lalu mengalami penyesuaian ke bentuk yang akan ditransmisikan $x_2(t)$, melewati kanal transmisi menjadi sinyal $x_3(t)$, diolah di *receiver* menjadi $x_4(t)$, dan menjadi bit-bit estimasi.

3.3 Skenario Simulasi Kanal Transmisi

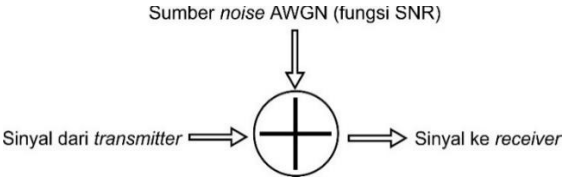
Simulasi sistem ADS-B dilakukan dalam 3 skenario kanal transmisi, yaitu skenario *point-to-point*, skenario kanal AWGN, dan skenario kanal Rayleigh. Simulasi ini dilakukan untuk melihat performa sistem ADS-B yang disimulasikan, baik tanpa tambahan algoritma enkripsi maupun dengan tambahan algoritma enkripsi, melalui pengamatan nilai BER yang dibandingkan dengan teori.

3.3.1 Skenario *Point-to-point*

Simulasi *point-to-point* yang dimaksud adalah simulasi dengan kanal yang tidak memberikan atenuasi terhadap amplitudo sinyal dan tidak ada penambahan *noise* pada sinyal. Simulasi ini bertujuan untuk memberikan kanal yang ideal untuk menganalisa performa algoritma enkripsi yang diaplikasikan. Skenario ini bertujuan untuk memastikan apakah Algoritma Blowfish yang disisipkan ke dalam keseluruhan sistem ADS-B telah bekerja sesuai desain, yaitu dengan menguji ketepatan proses enkripsi/dekripsi, perhitungan *Avalanche Effect*, perhitungan Koefisien Korelasi, dan perhitungan waktu pemrosesan informasi yang detailnya akan dibahas di subsubbab selanjutnya.

3.3.2 Skenario Kanal AWGN

Simulasi kanal AWGN dilakukan sesuai dengan diagram blok berikut.



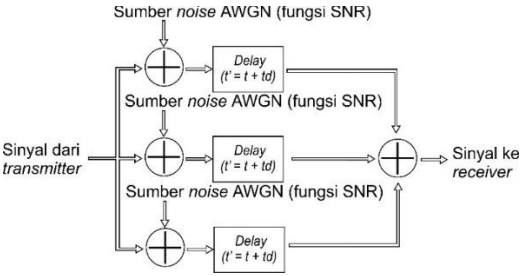
Gambar 3.7 Diagram Blok Simulasi Kanal AWGN

Sesuai dengan Gambar 3.6, pada simulasi kanal AWGN yang dilakukan, sinyal informasi yang sudah berbentuk pulsa-pulsa rektangular akan mendapat tambahan *noise* AWGN dari sebuah sumber *noise* AWGN. Sinyal inilah yang diterima oleh *receiver* ADS-B untuk diolah lebih lanjut.

Untuk mendapatkan nilai BER (*Bit Error Rate*) transmisi ADS-B di kanal AWGN, panjang sinyal ADS-B ditambah dengan menambah bit-bit informasi menjadi sejumlah 30000 bit dan melakukan simulasi dengan nilai SNR pada *range* 0 sampai 20, dengan perhitungan BER adalah sesuai rumus:

3.3.3 Skenario Kanal Rayleigh

Simulasi kanal Rayleigh dilakukan untuk melihat pengaruh adanya efek *multipath* pada siaran ADS-B sehingga terdapat tambahan siaran dengan *delay* yang kecil terhadap siaran utama. Simulasi dilakukan sesuai dengan model simulasi kanal Rayleigh yang dilakukan dalam referensi [12], yang digambarkan sebagai berikut.



Gambar 3.8 Diagram Blok Simulasi Kanal Rayleigh

Pada simulasi ini, diasumsikan suatu siaran ADS-B terbagi menjadi 3 *path* dimana siaran ADS-B pertama merupakan sinyal utama dan *path* kedua dan ketiga, dengan *delay* dan atenuasi tambahan masing-masing, akan mengganggu siaran di *path* pertama. Berdasarkan skenario tersebut, parameter yang digunakan untuk simulasi adalah sesuai Tabel 3.1.

Sinyal dari ketiga *path* dijumlah dan sinyal akhir inilah yang diterima oleh *receiver* ADS-B untuk diolah lebih lanjut. Untuk mendapatkan nilai BER transmisi ADS-B di kanal Rayleigh, panjang sinyal ADS-B ditambah dengan menambah bit-bit informasi menjadi sejumlah 30000 bit dan melakukan simulasi dengan nilai SNR pada *range* 0 sampai 20. Perhitungan BER dilakukan sesuai rumus (2.3).

Tabel 3.1 Parameter Simulasi Kanal Rayleigh

Path	*Delay*		Gain Tambahan (skala linier)	Keterangan
	Satuan sampel	Satuan waktu (mikrodetik)		
1	0	0	1	Siaran ADS-B utama
2	2	0,2	1/10	Siaran ADS-B yang terkena *delay*
3	3	0,3	1/2	Siaran ADS-B yang terkena *delay*

3.4 Perancangan Algoritma Enkripsi

Algoritma enkripsi yang diaplikasikan dalam simulasi ini adalah Algoritma Blowfish dengan blok data berukuran 8 bit, bukan 64 bit seperti standar Algoritma Blowfish. Algoritma Blowfish yang digunakan dalam simulasi telah disesuaikan agar berfungsi dengan tepat.

Untuk mengakomodir variasi jumlah bit informasi, maka sebelum memasuki komputasi Blowfish, bit-bit informasi disesuaikan dulu jumlahnya ke kelipatan 8 bit dengan penambahan zero padding di bagian akhir bit-bit informasi sehingga dapat diolah di Algoritma Blowfish 8 Bit yang dirancang. Sebagai contoh, informasi 5 bit akan ditambahkan 3 bit bernilai 0 sehingga panjangnya menjadi 8 bit dan informasi 25 bit akan ditambahkan 7 bit bernilai 0 sehingga panjangnya menjadi 32 bit.

Untuk mengakomodir perubahan ukuran blok data dari 64 bit menjadi 8 bit, maka dalam proses enkripsi maupun dekripsi, data yang

tadinya berbentuk matriks berukuran 1 x (jumlah bit informasi) akan diubah menjadi matriks dengan jumlah baris 8 dan jumlah kolom menyesuaikan sehingga proses enkripsi dan dekripsi dilakukan untuk tiap baris secara satu persatu.

Persiapan proses enkripsi diawali dengan inisialisasi yang bekerja sesuai *pseudocode* berikut.

Inisialisasi P-array[1x18] dan S-box[4x2] dengan nilai tetap (maksimum 4 bit dalam format binernya) yang diambil dari digit desimal Pi secara berurutan

Ubah nilai tiap anggota P-array & S-box ke biner sehingga P-array = 72 bit dan S-box[4x2] masing-masing 4 bit

Input Key dengan panjang diantara 1 – 56 bit

(Biner P-array) XOR (Biner Key yang diulang sampai sepanjang 72 bit)

Encrypt data bernilai 0 semua (8 bit) dengan Blowfish, *dengan P-array dan S-box yang ada*

Hasil enkripsi (8 bit) dipakai untuk menggantikan P1 (4 bit) dan P2 (4 bit)

Hasil enkripsi di-encrypt dengan Blowfish *lagi*

Hasil enkripsi terbaru dipakai untuk menggantikan P3 dan P4

Proses diulang sampai semua anggota P-array dan S-box diganti dengan nilai yang baru

Gambar 3.9 *Pseudocode* Inisialisasi Blowfish 8 Bit

Pemilihan nilai 56 bit (448 bit jika menuruti standar Blowfish dengan ukuran blok 64 bit) adalah sesuai dengan penskalaan, dimana 14 x 32 bit = 448 bit sesuai desain standar Blowfish diubah menjadi 14 x 4 bit = 56 bit agar bisa bekerja dengan ukuran blok 8 bit. Ukuran *S-box* juga

diubah sesuai dengan penskalaan dimana pada Blowfish standar (ukuran blok 64 bit), ukuran *S-box* adalah 4 baris x $2^{(64/8)}$ kolom = 4 baris x 256 kolom, sehingga untuk Blowfish dengan ukuran blok 8 bit, ukuran *S-box* menjadi 4 baris x $2^{(8/8)}$ kolom = 4 baris x 2 kolom.

Selanjutnya, Algoritma Blowfish digunakan untuk mengunci bit-bit informasi ADS-B.

Tabel 3.2 Ringkasan Penyesuaian Algoritma Blowfish

Blowfish standar	**Blowfish yang disimulasikan**
Ukuran blok = **64** bit (**32** bit kiri, **32** bit kanan)	Ukuran blok = **8** bit (**4** bit kiri, **4** bit kanan)
Panjang key maksimum = **448** bit = 14 × 32 bit	Panjang key maksimum = 14 × 4 bit = **56** bit
Ukuran S-box = 4 baris × $2^{(64/8)}$ kolom = **4 × 256**	Ukuran S-box = 4 baris × $2^{(8/8)}$ kolom = **4 × 2**

3.4.1 Integrasi Algoritma ke Sistem ADS-B

Algoritma Blowfish yang digunakan disisipkan di simulasi sistem ADS-B diantara Blok Bit stream *generator* dengan Blok *Transmitter* ADS-B, sehingga bit-bit informasi ADS-B akan dikunci terlebih dahulu sebelum dilakukan *mapping* dan penambahan *preamble* dan akhirnya ditransmisikan. Pada sisi penerima, Algoritma Blowfish disisipkan diantara Blok *Receiver* ADS-B dengan Blok Bit Estimasi sehingga bit estimasi tidak langsung diperoleh dari proses *demapping*, tetapi setelah *demapping* yang dilanjutkan dengan proses dekripsi.

Gambar 3.10 Integrasi Algoritma Enkripsi ke Sistem ADS-B

3.4.2 Skenario Pengukuran Performa Algoritma Enkripsi

Pengukuran performa algoritma enkripsi yang digunakan dilakukan dengan menguji validasi proses enkripsi dan dekripsi, mengukur nilai Avalanche Effect, mengukur nilai koefisien korelasi, dan mengukur waktu proses algoritma enkripsi.

3.4.2.1 *Validasi Proses Enkripsi dan Dekripsi*

Pengukuran ketepatan proses enkripsi dan dekripsi dilakukan dengan percobaan melakukan enkripsi dan dekripsi dengan Algoritma Blowfish 8 Bit untuk berbagai macam jumlah bit informasi, mulai dari 1 sampai 7 bit sebagai jumlah bit yang kurang dari ukuran blok data, 8 bit sebagai jumlah bit yang tepat sama dengan ukuran blok data, dan dengan jumlah bit diatas 8 bit sebagai jumlah bit yang lebih dari ukuran blok data.

Untuk simulasi dengan jumlah bit informasi 1-8 bit, jumlah bit informasi ditentukan sesuai ukuran yang ingin diuji dengan nilai 0 atau 1 yang dibangkitkan secara acak. Untuk simulasi dengan jumlah bit informasi diatas 8 bit, jumlah bit dan nilai 0 atau 1-nya dibangkitkan secara acak. Untuk setiap percobaan, panjang *key* dan nilai desimal *key* dibangkitkan secara acak, sesuai ketentuan masing-masing. Masing-masing percobaan dilakukan sebanyak 10 kali untuk melihat pengaruh variasi nilai informasi, panjang *key*, dan nilai desimal *key* terhadap ketepatan proses enkripsi dan dekripsi.

3.4.2.2 *Pengukuran Avalanche Effect*

Pengukuran *Avalanche Effect* [13,14] dilakukan di keseluruhan *round* dalam proses komputasi Algoritma Blowfish (16 *round*). Jumlah bit informasi yang dibangkitkan adalah 112 bit, sesuai format *frame* ADS-B, yang nilai 0 atau 1-nya dibangkitkan secara acak. Pada pengukuran ini, *plaintext* diatur tetap. Yang diubah adalah nilai *key* yaitu dari awalnya diatur senilai 2^{55} diubah menjadi $2^{55} + 2^{54}$, dengan panjang *key* diatur tetap sepanjang 56 bit. Pengukuran *Avalanche Effect* dilakukan sebanyak 20 kali sesuai Gambar 3.11.

```
Inisialisasi format frame ADS-B (112 bit)
Inisialisasi panjang key = 56
Inisialisasi kunci 1 =2^55 dan kunci 2 = 2^55 + 2^54
Untuk i = 1:2
    Inisialisasi Algoritma Blowfish 8 bit dengan kunci ke-i
    Untuk j = 1 sampai 16
            Simpan bit-bit hasil enkripsi round ke-j di matriks-i
    selesai
selesai
Hitung perbedaan bit-bit di tiap round saat dikunci dengan kunci 1 dan saat
dikunci kunci 2
```

Gambar 3.11 *Pseudocode* Pengukuran *Avalanche Effect*

3.4.2.3 *Pengukuran Koefisien Korelasi*

Pengukuran Koefisien Korelasi [13] diawali dengan membangkitkan bit informasi sejumlah 112 bit, sesuai format *frame* ADS-B, yang nilai 0 atau 1-nya dibangkitkan secara acak. Panjang *key* dan nilai *key* dibangkitkan secara acak sesuai dengan ketentuannya masing-masing. Pengukuran nilai Koefisien Korelasi dilakukan sebanyak 100 kali sesuai dengan Gambar 3.12.

Inisialisasi x = format frame ADS-B (112 bit)

Inisialisasi panjang key (acak, antara 1 – 56)

Inisialisasi nilai desimal kunci (acak, antara 0 sampai $2^{(panjang\ key-1)}$)

Inisialisasi Algoritma Blowfish *8 bit dengan kunci*

Encrypt x dengan Algoritma Blowfish, *menghasilkan cipher*

Hitung Koefisien Korelasi antara x dengan cipher dengan fungsi corr pada MATLAB

Gambar 3.12 *Pseudocode* Pengukuran Koefisien Korelasi

3.4.2.4 *Pengukuran Waktu Proses*

Pengukuran durasi persiapan enkripsi dan durasi dekripsi diawali dengan membangkitkan 112 bit informasi sesuai format *frame* ADS-B, dengan nilai 0 atau 1-nya dibangkitkan secara acak. Panjang *key* dan nilai desimal *key* juga dibangkitkan secara acak, sesuai ketentuan masing-masing. Pengukuran durasi komputasi yang terjadi dilakukan dengan menggunakan fungsi *tic* dan *toc* sebagai fungsi pengukur durasi di dalam program MATLAB sesuai Gambar 3.13. Untuk memperoleh analisa yang tepat, dilakukan juga pengukuran durasi pengolahan sinyal dalam sistem tanpa penambahan Algoritma Blowfish (hanya *demapping* pulsa ke bit saja). Pengukuran dilakukan sebanyak 100 kali sesuai dengan Gambar 3.14. Selain itu, hasil pengukuran ini dijadikan dasar perhitungan waktu untuk proses *cryptanalysis* terhadap *brute force attack*.

Inisialisasi format frame ADS-B (112 bit)
Inisialisasi panjang key (acak, antara 1 – 56)
Inisialisasi nilai desimal kunci (acak, antara 0 sampai $2^{(panjang\ key-1)}$*)*

tic
Inisialisasi Algoritma Blowfish *8 bit dengan kunci*
toc

Encrypt informasi dengan Algoritma Blowfish
Mapping bit-bit ke pulsa PPM

tic
Demapping pulsa PPM ke bit-bit
toc
tic
Decrypt informasi dengan Algoritma Blowfish
toc

Gambar 3.13 *Pseudocode* Pengukuran Durasi Setelah Penambahan Blowfish

Inisialisasi format frame ADS-B (112 bit)
Mapping bit-bit ke pulsa PPM

tic
Demapping pulsa PPM ke bit-bit
toc

Gambar 3.14 *Pseudocode* Pengukuran Durasi Sebelum Penambahan Blowfish

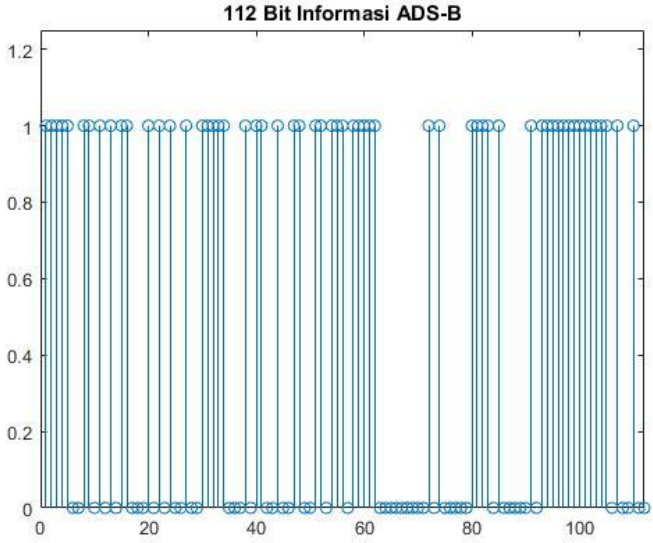
Halaman ini sengaja dikosongkan

BAB 4
ANALISA HASIL SIMULASI

4.1 Hasil Simulasi Sistem ADS-B dengan Blowfish 8 Bit

Sistem ADS-B dengan penambahan algoritma enkripsi Blowfish 8 Bit yang disimulasikan bekerja sesuai dengan model yang dijelaskan di subbab 3.1 dan 3.4, dengan penjelasan sebagai berikut.

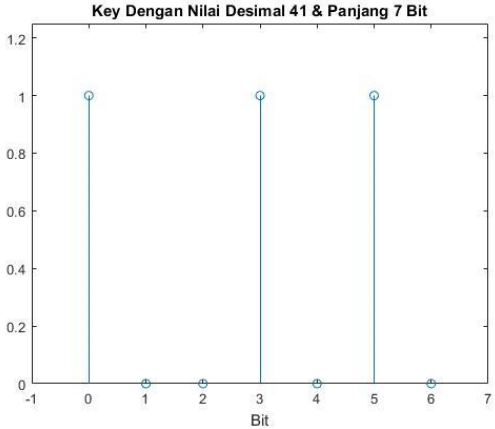
Pertama-tama, *frame generator* membangkitkan 112 bit informasi yang terbagi dalam 4 kelompok yaitu 8 bit *Control*, 24 bit *ICAO Address*, 56 bit pesan ADS-B, dan 24 bit *parity*, yang dalam simulasi ini nilai 0 atau 1-nya dibangkitkan secara acak.



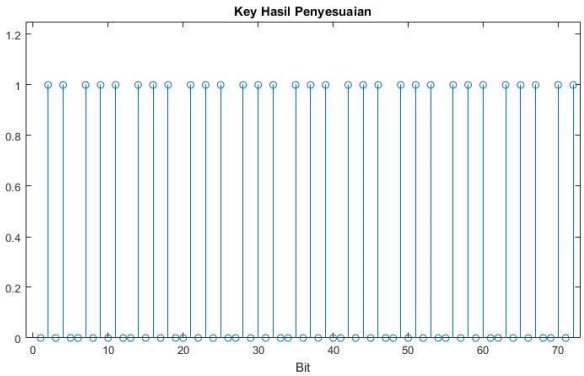
Gambar 4.1 112 Bit Informasi ADS-B

Selanjutnya adalah proses enkripsi dengan Algoritma Blowfish 8 Bit. Dalam simulasi, panjang bit *key* dan nilai desimal *key* dibangkitkan secara acak, seperti yang ditunjukkan Gambar 4.2. Untuk melakukan persiapan enkripsi, dilakukan update *P-array* dan *S-box*, dengan *key* dimodifikasi (bit-bit *key* diulang hingga mencapai nilai 72 bit; jika lebih,

maka diambil bit ke 1 hingga 72 saja) menjadi sepanjang 72 bit untuk mengacak *P-array*, seperti yang ditunjukkan Gambar 4.3.

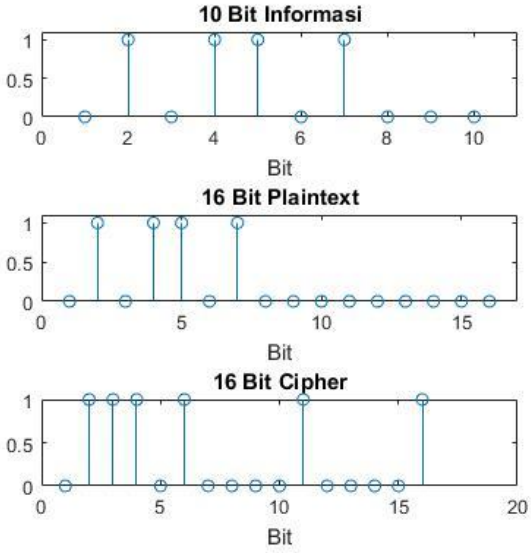


Gambar 4.2 Biner *Key* Asli

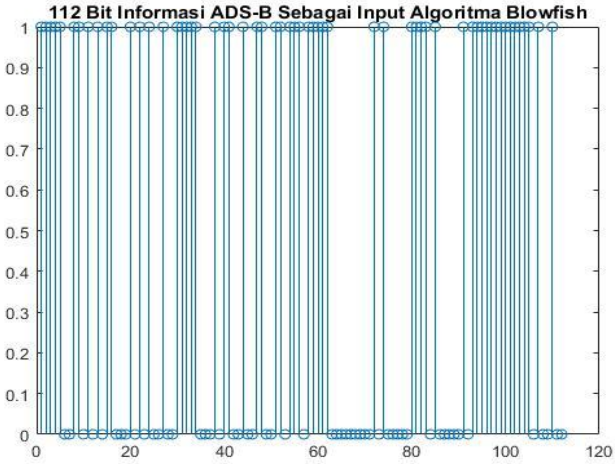


Gambar 4.3 Biner *Key* Hasil Penyesuaian

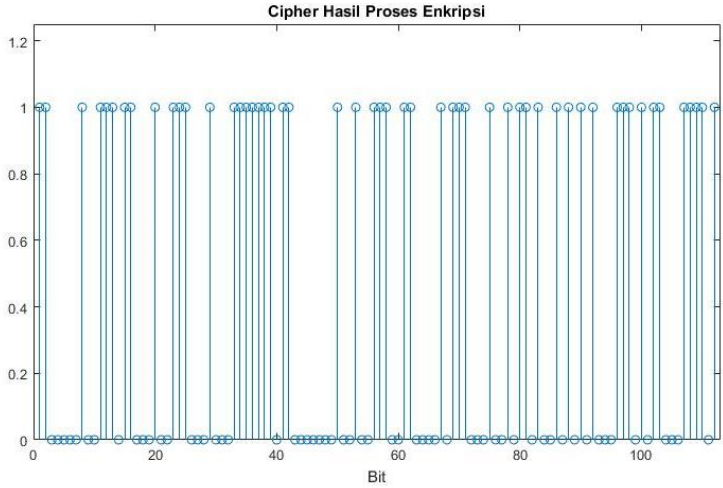
Kemudian 112 bit informasi yang dibangkitkan sebelumnya dikunci menggunakan Algoritma Blowfish 8 Bit yang sudah siap melakukan enkripsi. Karena panjang bit informasi merupakan kelipatan 8, tidak diperlukan penyesuaian panjang bit informasi ke jumlah bit kelipatan 8 seperti yang ditunjukkan Gambar 4.4.



Gambar 4.4 Proses Enkripsi 10 Bit Informasi

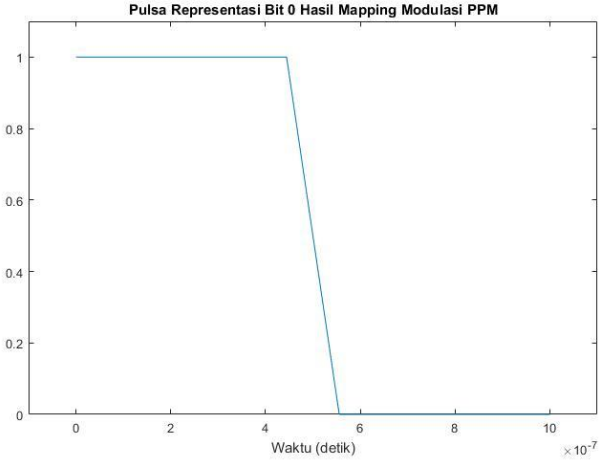


Gambar 4.5 112 Bit Informasi ADS-B Sebagai Input Blowfish

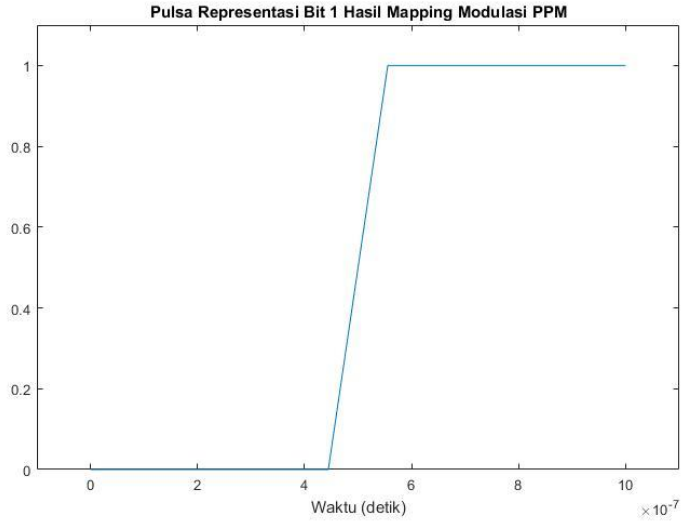


Gambar 4.6 112 Bit *Cipher* Hasil Enkripsi

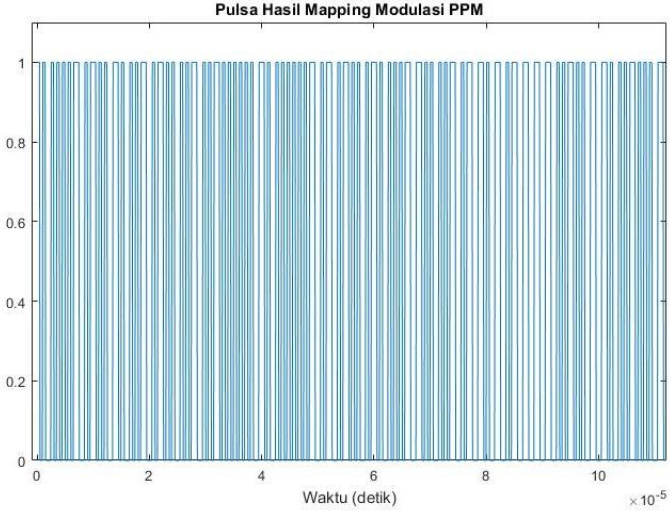
Tahapan selanjutnya adalah *mapping* bit-bit informasi ke pulsa-pulsa PPM. Gambar 4.7 – 4.9 menunjukkan pulsa representasi bit 0, bit 1, dan pulsa hasil *mapping* 112 bit informasi ADS-B dari bit-bit aslinya..



Gambar 4.7 Pulsa Bit 0

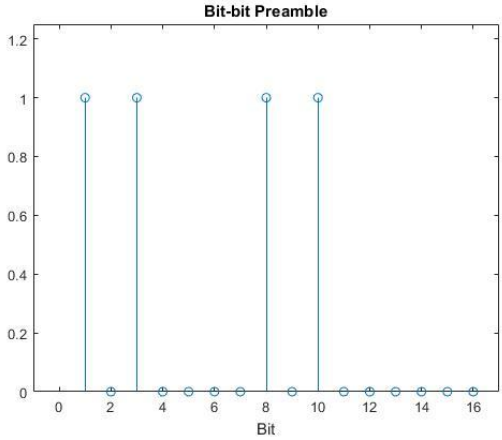


Gambar 4.8 Pulsa Bit 1

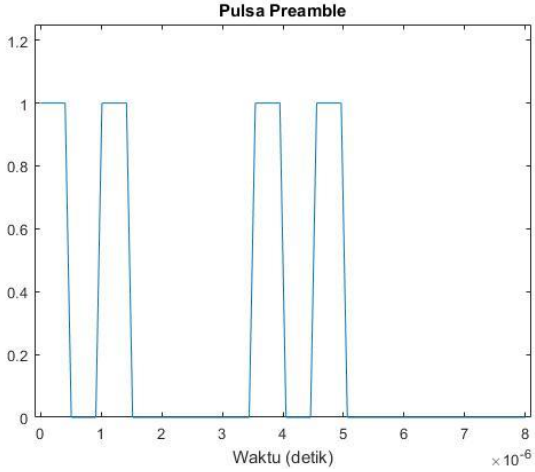


Gambar 4.9 Pulsa PPM Informasi ADS-B

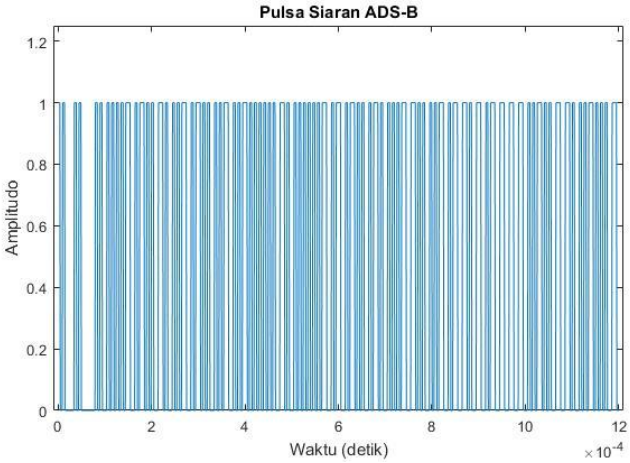
Kemudian, pulsa-pulsa PPM diberi tambahan pulsa *preamble* yang berada di bagian depan dari susunan pulsa siaran ADS-B dan dilepaskan ke udara dan memasuki kanal transmisi.



Gambar 4.10 Bit *Preamble*

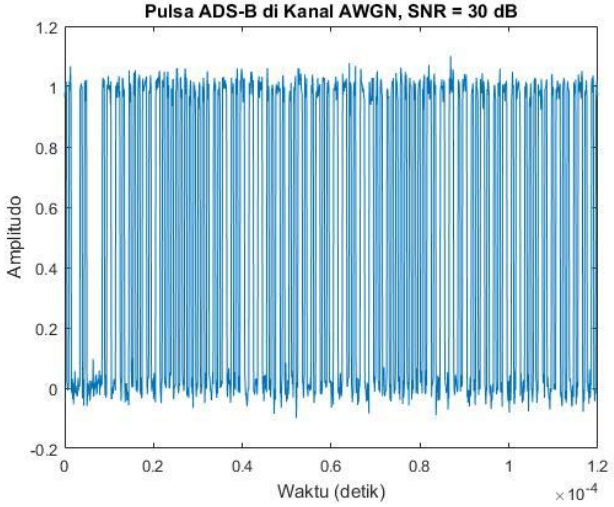


Gambar 4.11 Pulsa *Preamble*

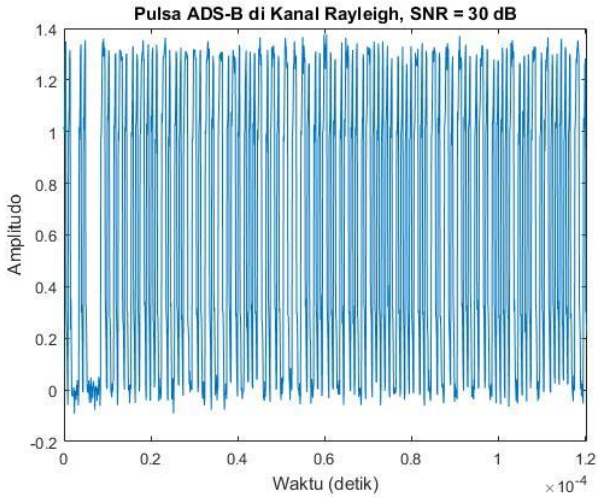


Gambar 4.12 Pulsa Siaran ADS-B

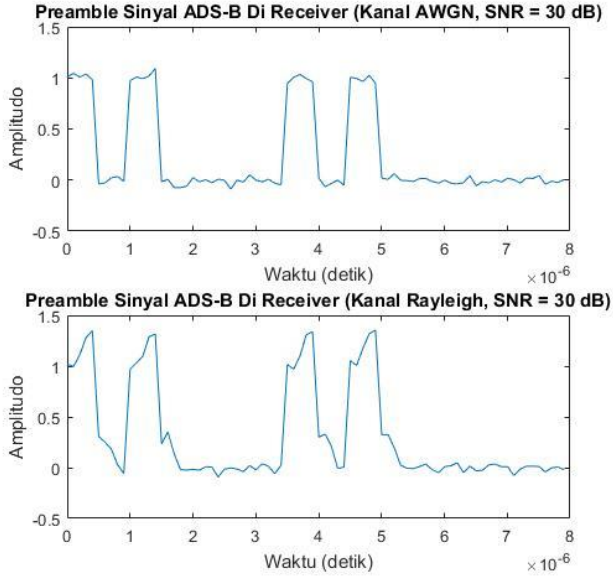
Pada kanal transmisi, pulsa-pulsa siaran ADS-B terkena tambahan *noise*, sesuai dengan model kanal transmisi yang disimulasikan, yaitu kanal AWGN dan kanal Rayleigh.



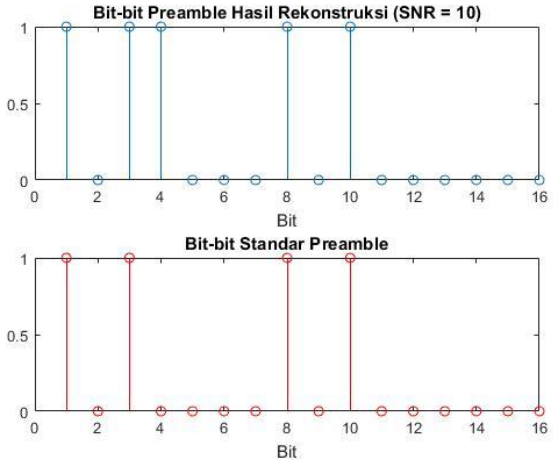
Gambar 4.13 Pulsa Siaran ADS-B di Kanal AWGN



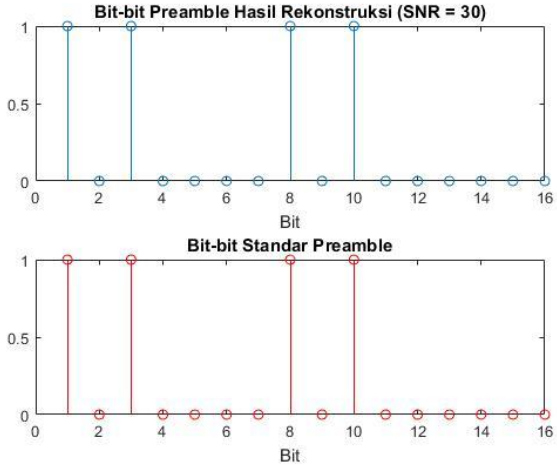
Gambar 4.14 Pulsa Siaran ADS-B di Kanal Rayleigh



Gambar 4.15 Pulsa *Preamble* di *Receiver*



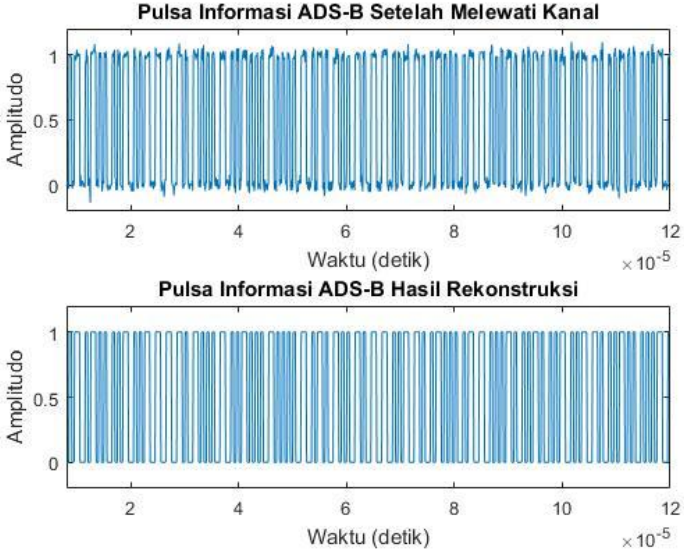
Gambar 4.16 Perbandingan Pulsa *Preamble* Hasil Rekonstruksi dengan Pulsa *Preamble* Standar untuk SNR = 10 dB



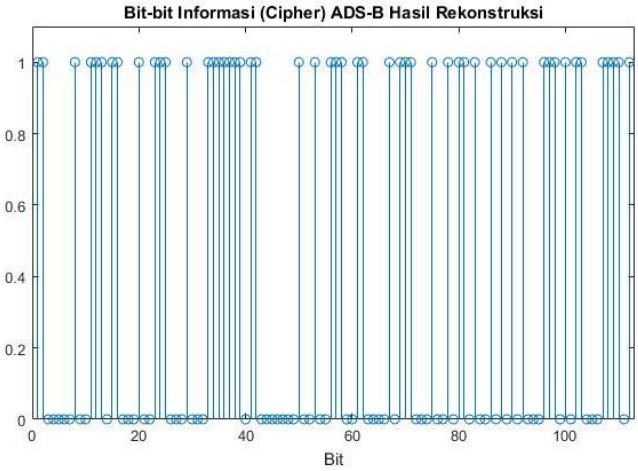
Gambar 4.17 Perbandingan Pulsa *Preamble* Hasil Rekonstruksi dengan Pulsa *Preamble* Standar untuk SNR = 30 dB

Pulsa-pulsa yang telah melewati kanal kemudian diterima oleh penerima ADS-B dan dilakukan proses mengenali *preamble* untuk memastikan keabsahan sinyal yang diterima. Untuk mengenali *preamble*, pulsa-pulsa *preamble* dipisahkan dari keseluruhan sinyal yang diterima, diperbaiki bentuknya, kemudian diterjemahkan kembali ke bentuk bit-bit untuk dibandingkan dengan bit-bit *preamble* standar.

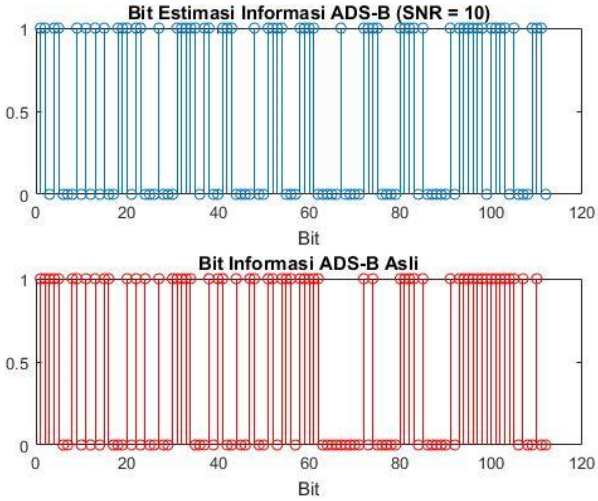
Setelah *preamble* dikenali, pulsa-pulsa yang berisi informasi ADS-B diperbaiki bentuk pulsanya, kemudian dilakukan *demapping* kembali ke bit-bit informasi, atau lebih tepatnya bit-bit *cipher* yang harus "dibuka" kembali dengan Algoritma Blowfish 8 Bit. Dengan menggunakan kunci yang sama dengan yang digunakan untuk melakukan enkripsi, bit-bit estimasi informasi ADS-B dihasilkan.



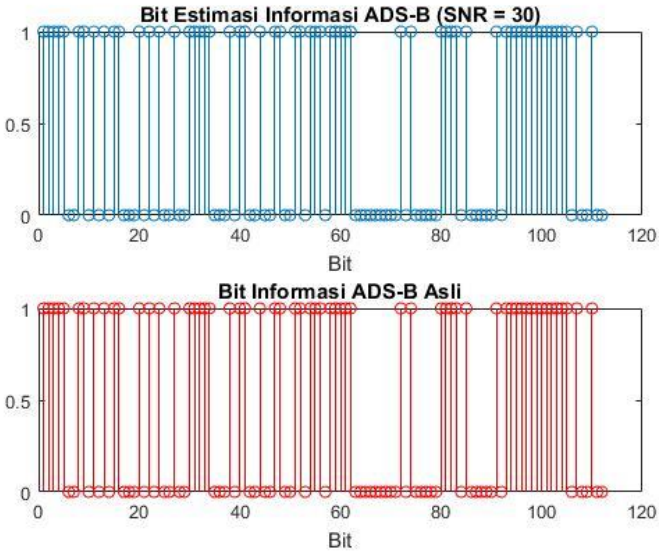
Gambar 4.18 Rekonstruksi Pulsa Informasi ADS-B



Gambar 4.19 Bit-bit Informasi Hasil *Demapping*



Gambar 4.20 Perbandingan Bit Estimasi dengan Bit Asli, SNR = 10dB



Gambar 4.21 Perbandingan Bit Estimasi dengan Bit Asli, SNR = 30 dB

4.2 Hasil Simulasi Algoritma Enkripsi

Untuk mengukur performa Algoritma Enkripsi, simulasi dilakukan sesuai dengan skenario pada subbab 3.4. Pengujian dilakukan untuk melihat apakah Algoritma Blowfish 8 Bit yang dirancang berhasil melakukan proses enkripsi dan dekripsi untuk jumlah bit yang bervariasi, dengan nilai panjang bit *key* dan nilai desimal *key* yang dibangkitkan secara acak. Hasil simulasi per skenario dan pembahasannya akan dijelaskan di bagian selanjutnya.

4.2.1 Jumlah Bit Informasi Kurang Dari 8 Bit

Pengujian dilakukan untuk bit informasi kurang dari 8 bit, yaitu 1 hingga 7 bit, dimana diperlukan penambahan *zero padding* agar bit informasi menjadi sepanjang 8 bit sehingga sesuai dengan ukuran blok data Algoritma Blowfish yang digunakan. Tabel 4.1 menunjukkan nilai panjang bit *key*,nilai desimal *key*, dan status keberhasilan pengujian.

Tabel 4.1 Hasil Simulasi Enkripsi/Dekripsi Kurang Dari 8 Bit

Bit Informasi	Percobaan	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/ Dekripsi
1	1	18	23.448	Sukses
	2	10	389	Sukses
	3	20	41.189	Sukses
	4	15	6.083	Sukses
	5	2	1	Sukses
	6	51	142.974.444.635.100	Sukses
	7	31	1.028.115.136	Sukses
	8	9	249	Sukses
	9	24	7.681.747	Sukses
	10	2	2	Sukses
2	1	23	117.521	Sukses
	2	17	902	Sukses
	3	10	59	Sukses
	4	31	788.906.375	Sukses
	5	52	1.607.772.218.459.260	Sukses
	6	43	3.268.331.158.725	Sukses
	7	10	362	Sukses
	8	3	0	Sukses
	9	18	124.548	Sukses
	10	22	1.605.405	Sukses
3	1	27	32.123.525	Sukses
	2	2	0	Sukses
	3	2	1	Sukses
	4	16	27.250	Sukses

Bit Informasi	Percobaan	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/ Dekripsi
	5	25	12.856.004	Sukses
	6	25	10.843.333	Sukses
	7	39	180.071.968.176	Sukses
	8	43	1.121.920.182.545	Sukses
	9	17	6.887	Sukses
	10	53	197.023.344.759.363	Sukses
4	1	24	4.581.434	Sukses
	2	9	222	Sukses
	3	17	63.512	Sukses
	4	25	9.235.254	Sukses
	5	33	4.173.431.266	Sukses
	6	22	217.797	Sukses
	7	44	828.733.903.353	Sukses
	8	32	209.156.111	Sukses
	9	4	0	Sukses
	10	12	154	Sukses
5	1	33	3.893.393.967	Sukses
	2	21	745.904	Sukses
	3	51	230.432.168.184.021	Sukses
	4	12	1.660	Sukses
	5	15	14.989	Sukses
	6	8	3	Sukses
	7	8	7	Sukses
	8	25	544.987	Sukses

Bit Informasi	Percobaan	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/ Dekripsi
	9	11	17	Sukses
	10	36	1.507.328.998	Sukses
6	1	42	1.883.746.946.211	Sukses
	2	11	78	Sukses
	3	17	9.715	Sukses
	4	39	21.522.303.047	Sukses
	5	2	1	Sukses
	6	16	1.709	Sukses
	7	51	51.966.864.558.148	Sukses
	8	10	61	Sukses
	9	4	0	Sukses
	10	19	24.402	Sukses
7	1	30	406.721.036	Sukses
	2	25	4.417.095	Sukses
	3	32	1.146.835.857	Sukses
	4	26	17.538.998	Sukses
	5	24	3.467.976	Sukses
	6	53	436.687.416.290.922	Sukses
	7	46	2.833.741.104.540	Sukses
	8	36	2.521.337.807	Sukses
	9	13	116	Sukses
	10	10	19	Sukses

Berdasarkan data dari tabel 4.1, terlihat bahwa variasi panjang bit *key* dan nilai desimal *key* tidak mempengaruhi keberhasilan proses enkripsi dan dekripsi dari Algoritma Blowfish 8 bit hasil rancangan.

4.2.2 Jumlah Bit Informasi Tepat 8 Bit

Pengujian dilakukan untuk bit informasi tepat 8 bit dimana tidak diperlukan penambahan *zero padding* karena bit informasi sudah sepanjang 8 bit dan sudah sesuai dengan ukuran blok data Algoritma Blowfish yang digunakan. Tabel 4.2 menunjukkan nilai panjang bit *key*, nilai desimal *key*, dan status keberhasilan pengujian.

Tabel 4.2 Hasil Simulasi Enkripsi/Dekripsi Tepat 8 Bit

Bit Informasi	Percobaan	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/ Dekripsi
8	1	26	22.962.854	Sukses
	2	52	1.018.453.208.344.416	Sukses
	3	22	2.052.957	Sukses
	4	12	1.690	Sukses
	5	13	527	Sukses
	6	42	134.307.812.033	Sukses
	7	37	5.833.729.875	Sukses
	8	17	2.747	Sukses
	9	51	125.386.195.578.755	Sukses
	10	36	2.652.856.943	Sukses

Berdasarkan data dari tabel 4.2, terlihat bahwa variasi panjang bit *key* dan nilai desimal *key* tidak mempengaruhi keberhasilan proses enkripsi dan dekripsi dari Algoritma Blowfish 8 bit hasil rancangan.

4.2.3 Jumlah Bit Informasi Lebih Dari 8 Bit

Pengujian dilakukan untuk bit informasi dengan jumlah lebih dari 8 bit dimana mungkin diperlukan penambahan *zero padding* agar panjang informasi menjadi kelipatan dari 8 dan pembagian bit-bit informasi menjadi blok-blok berukuran 8 bit agar sesuai dengan ukuran blok data Algoritma Blowfish yang digunakan.

4.2.3.1 *Jumlah Bit Informasi Bukan Kelipatan 8*

Panjang bit informasi yang lebih dari 8 bit dan bukan kelipatan 8 menyebabkan perlunya penambahan *zero padding* agar panjang bit informasi mencapai kelipatan 8 sehingga sesuai dengan ukuran blok Algoritma Blowfish yang digunakan. Hasil simulasi ditunjukkan di Tabel 4.3.

Tabel 4.3 Hasil Simulasi Enkripsi/Dekripsi Lebih Dari 8 Bit (Bukan Kelipatan 8)

Bit Informasi	Bit Informasi Hasil Penyesuaian	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/ Dekripsi
34	40	45	1.193.678.395.613	Sukses
119	120	19	28.790	Sukses
1.001	1.008	9	6	Sukses
2.974	2.976	38	3.432.482.009	Sukses
3.403	3.408	34	925.262.863	Sukses
3.572	3.576	50	48.156.575.567.281	Sukses
10.340	10.344	55	1.972.885.637.678.804	Sukses
12.305	12.312	32	75.261.703	Sukses
13.733	13.736	18	38.476	Sukses
15.773	15.776	48	9.114.452.079.599	Sukses

Berdasarkan data dari tabel 4.3, terlihat bahwa variasi jumlah bit informasi, panjang bit *key* dan nilai desimal *key* tidak mempengaruhi keberhasilan proses enkripsi dan dekripsi dari Algoritma Blowfish 8 bit hasil rancangan.

4.2.3.2 *Jumlah Bit Informasi Kelipatan 8*

Panjang bit informasi yang lebih dari 8 bit dan kelipatan 8 menyebabkan tidak perlunya penambahan *zero padding* karena panjang bit informasi merupakan kelipatan 8 sehingga sudah sesuai dengan ukuran blok Algoritma Blowfish yang digunakan. Hasil simulasi ditunjukkan di Tabel 4.4.

Tabel 4.4 Hasil Simulasi Enkripsi/Dekripsi Lebih Dari 8 Bit (Kelipatan 8)

Bit Informasi	Panjang *Key* (bit)	Nilai Desimal *Key*	Keberhasilan Enkripsi/Dekripsi
1.440	54	824.314.564.994.558	Sukses
3.672	29	28.156.150	Sukses
4.840	40	36.618.439.993	Sukses
5.184	51	52.033.592.449.925	Sukses
7.216	16	1.064	Sukses
10.528	50	64.019.613.747.871	Sukses
11.496	54	115.534.381.833.496	Sukses
15.952	11	99	Sukses
16.232	54	1.077.000.093.064.905	Sukses
16.688	13	407	Sukses

Berdasarkan data dari tabel 4.4, dapat disimpulkan bahwa variasi jumlah bit informasi, panjang bit *key* dan nilai desimal *key* tidak mempengaruhi keberhasilan proses enkripsi dan dekripsi dari Algoritma Blowfish 8 bit hasil rancangan.

4.3 Analisa Keamanan Informasi

Hasil simulasi untuk pengujian keamanan informasi hasil enkripsi dengan Algoritma Blowfish 8 bit hasil rancangan memberikan gambaran mengenai tingkat kekuatan algoritma enkripsi yang diterapkan dalam simulasi. Data hasil simulasi untuk setiap skenario dan pembahasannya akan dibahas di bagian selanjutnya.

4.3.1 Perhitungan *Avalanche Effect*

Perhitungan nilai *Avalanche Effect* bertujuan untuk melihat seberapa banyak bit yang berubah pada setiap *round* Algoritma Blowfish 8 Bit yang digunakan akibat perubahan 1 bit pada *key*. Hasil perhitungan *Avalanche Effect* yang didapat dari simulasi sesuai skenario di subbab 3.4 adalah sebagai berikut.

Tabel 4.5 Rata-rata Hasil Perhitungan *Avalanche Effect*

Round	Hasil Pengukuran	
	Rata-rata Perubahan Jumlah Bit	Rasio
1	1,3	0,1625
2	2,85	0,35625
3	2,55	0,31875
4	3	0,375
5	2,7	0,3375
6	3,75	0,46875
7	2,55	0,31875
8	1	0,125
9	2,7	0,3375
10	4,15	0,51875
11	3,45	0,43125
12	3	0,375
13	2,3	0,2875
14	2,85	0,35625
15	2,55	0,31875
16	4	0,5

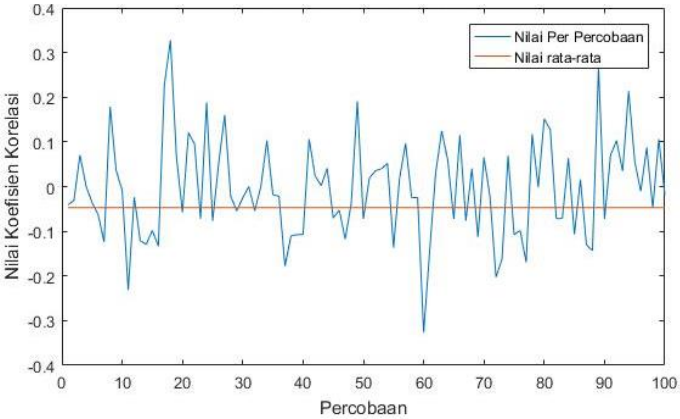
Dengan membandingkan tabel hasil pengukuran dengan teori *Avalanche Effect*, dapat disimpulkan bahwa *round* 8 merupakan *round* dengan tingkat keamanan paling rendah karena memiliki nilai rata-rata 12,5% bit *cipher* saja yang berubah dan *round* 10 merupakan *round* dengan tingkat keamanan paling tinggi karena rata-rata 51,875% *cipher* berubah dengan hanya merubah 1 bit pada *key*.

Secara keseluruhan, performa Algoritma Blowfish 8 bit hasil rancangan dikatakan baik dengan 2 *round* memiliki rasio *Avalanche Effect* lebih besar atau sama dengan 50%, dengan rata-rata *Avalanche Effect* dalam keseluruhan proses enkripsi oleh Algoritma Blowfish 8 Bit rancangan (*round* 1 hingga 16) sebesar 34,922%.

4.3.2 Perhitungan Koefisien Korelasi

Perhitungan nilai Koefisien Korelasi bertujuan untuk mengukur berapa nilai korelasi linier antara *plaintext* dengan *cipher* Algoritma Blowfish 8 Bit yang digunakan. Dengan mengetahui nilai korelasi linier

antara *plaintext* dengan *cipher*, akan didapatkan gambaran mengenai kekuatan algoritma enkripsi yang digunakan, dimana dikarapkan korelasi linier antara *plaintext* dengan *cipher* bernilai mendekati 0 sehingga *cryptanalysis* tidak mudah dilakukan. Hasil perhitungan Koefisien Korelasi yang didapat dari simulasi sesuai skenario di sub bab 3.4 adalah sebagai berikut.



Gambar 4.22 Grafik Koefisien Korelasi

Tabel 4.6 Data Statistik Koefisien Korelasi

Jenis Data	Nilai
Rata-rata	-0,004716
Standar Deviasi	0,111474
Nilai Maksimum	0,3273
Nilai Minimum	-0,3267
Jumlah Data Kategori Korelasi Lemah	98
Jumlah Data Kategori Korelasi Sedang	2

Berdasarkan data di Tabel 4.6, dapat disimpulkan bahwa mayoritas nilai Koefisien Korelasi antara *cipher* dengan *plaintext* dari Algoritma Blowfish 8 bit hasil rancangan (98 dari 100 percobaan) masuk ke kategori korelasi linier rendah, dengan 2 hasil percobaan lainnya masuk ke kategori korelasi linier sedang. Dengan demikian, dapat dikatakan bahwa performa Algoritma Blowfish 8 bit hasil rancangan adalah baik.

4.3.3 Hasil *Cryptanalysis*

Cryptanalysis untuk Algoritma Blowfish 8 bit didasarkan pada cyptanalysis yang dilakukan pada penelitian sebelumnya sesuai referensi [9]. Sesuai dengan definisinya, *brute force attack* dilakukan dengan mencoba semua kombinasi kunci yang mungkin digunakan pada algoritma enkripsi yang diuji. Referensi [9] memberikan penjelasan mengenai *cryptanalysis* Algoritma Blowfish 64 Bit dengan 2^{448} kemungkinan kunci, namun tidak menjelaskan dengan rinci metode pengukuran durasi *brute force attack* yang dilakukan. Oleh karena itu pada penelitian ini, perhitungan durasi total *brute force attack* dilakukan dengan menggunakan pengukuran menggunakan data hasil simulasi sesuai subbab 3.4 dan perhitungan dilakukan sesuai rumus (2.1).

Hasil simulasi menunjukkan adanya fluktuasi pada durasi dekripsi menggunakan Algoritma Blowfish 8 bit. Fluktuasi ini disebabkan oleh sifat *syntax* yang digunakan dalam pengukuran, yaitu *tic* dan *toc*, yang saat dijalankan akan mengukur *wall clock time*, sehingga durasi terukur adalah durasi proses dalam simulasi yang dilakukan ditambah durasi proses-proses lain yang berjalan pada komputer tempat simulasi dilakukan, baik aplikasi selain program simulasi maupun proses-proses *background* sehingga tidak menunjukkan durasi pengolahan sinyal informasi yang sebenarnya. Hasil terbaik yang dapat diasumsikan sebagai durasi dekripsi adalah waktu dekripsi minimal, yaitu 0,05794 detik, yang merupakan durasi dekripsi dengan 1 *key*. Pada Algoritma Blowfish 8 bit yang digunakan, terdaapt 2^{56} kemungkinan *key* sehingga total waktu untuk *brute force attack* adalah selama $4{,}175017 \times 10^{15}$ detik atau mencapai lebih dari 132 juta tahun, ditambah dengan waktu untuk menentukan mana informasi yang tepat dari seluruh kemungkinan informasi hasil dekripsi.

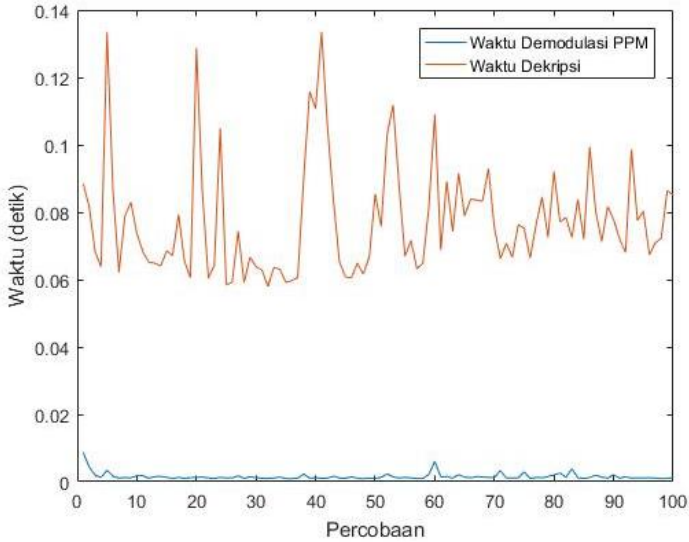
Total waktu percobaan selama itu menunjukkan bahwa usaha untuk mendapatkan informasi mengenai pesawat yang sedang dalam perjalanan, seperti posisi, kecepatan, dan ketinggian pesawat untuk dimanfaatkan secara *real-time* tidak sebanding dengan hasilnya karena proses memperoleh informasi yang terlalu lama. Kesimpulan yang diperoleh adalah Algoritma Blowfish 8 Bit hasil rancangan dalam Tugas Akhir ini memberikan perlindungan yang baik kepada pesan ADS-B yang disiarkan oleh pesawat terhadap serangan *brute force attack* yang dilakukan menggunakan komputer dengan spesifikasi sama seperti komputer yang digunakan untuk penelitian ini.

4.4 Hasil Pengukuran Waktu Proses

Hasil pengukuran durasi beberapa tahapan dalam simulasi yang dilakukan sesuai skenario di subbab 3.4 memberikan gambaran mengenai dampak penambahan algoritma enkripsi ke performa sistem ADS-B untuk memberikan gambaran mengenai pengaruh adanya tambahan proses dekripsi dengan Algoritma Blowfish 8 Bit selain adanya proses *demapping* pulsa PPM ke bit estimasi.

Tabel 4.7 Data Statistik Pengukuran Waktu Proses

Jenis Nilai	Waktu Proses Sebelum Penambahan Algoritma Blowfish (detik)	Waktu Proses Setelah Penambahan Algoritma Blowfish (detik)		
		Durasi Demodulasi	Durasi Dekripsi	Total
Maksimum	0,001879	0,008688	0,133460	0,142148
Minimum	0,000401	0,000886	0,057940	0,058827
Rata-rata	0,000752	0,001533	0,077554	0,079088



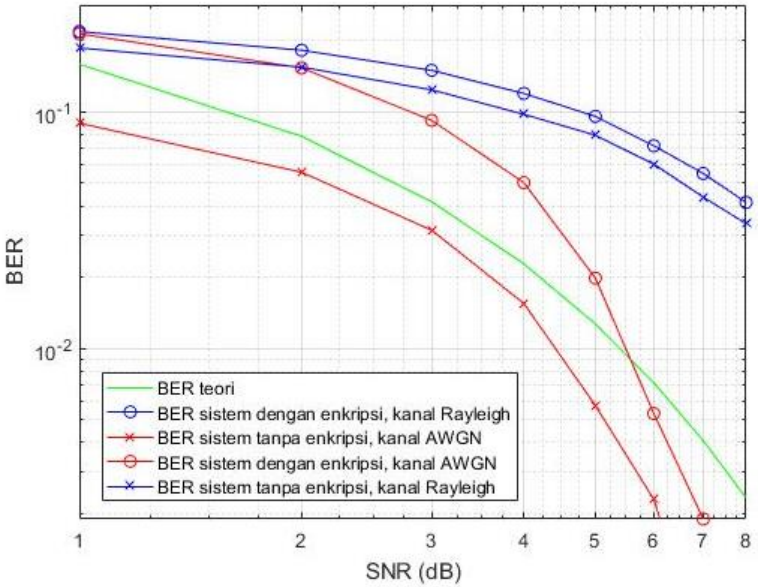
Gambar 4.23 Grafik Durasi Pengolahan Sinyal Informasi

Hasil pengukuran menunjukkan adanya fluktuasi pada durasi pengolahan sinyal informasi akibat sifat dari *syntax tic* dan *toc* yang

mengukur *wall clock time*, sehingga hasil pengukuran bukanlah durasi proses yang sebenarnya. Hasil pengukuran terbaik yang dapat diasumsikan sebagai durasi pengolahan sinyal informasi adalah nilai terkecil yang diperoleh, yaitu 0,000886 detik untuk proses demodulasi dan 0,05794 detik untuk dekripsi informasi.

4.5. Perbandingan Performa Pada Kanal AWGN dan Rayleigh

Performa sistem ADS-B diuji di kanal transmisi untuk melihat performa sistem ADS-B yang dirancang. Pengujian dilakukan sesuai dengan model yang dijelaskan di subbab 3.3, yaitu di kanal AWGN dan kanal Rayleigh. Pengamatan dilakukan terhadap pengaruh perubahan nilai SNR terhadap nilai BER yang didapat dari simulasi di kedua jenis kanal transmisi, dengan sistem ADS-B yang ditambahkan Algoritma Blowfish 8 bit maupun yang tidak ditambahkan algoritma enkripsi. Hasil simulasi dapat dilihat di grafik berikut.



Gambar 4.24 Grafik BER Kanal AWGN & Rayleigh

Berdasarkan grafik tersebut, semakin tinggi nilai SNR, semakin rendah nilai BER atau dengan kata lain semakin tinggi nilai SNR, performa sistem ADS-B semakin baik. Namun, secara umum dapat terlihat bahwa terdapat perbedaan antara BER hasil simulasi dengan BER pada teori [15]. Hal ini disebabkan karena *plot* BER sesuai teori adalah berdasarkan rumus matematis sementara pada simulasi, *plot* BER ditentukan oleh pemodelan sistem yang dibuat. Adanya perbedaan *plot* menunjukkan pemodelan yang dibuat belum sempurna.

Selain itu dapat dilihat bahwa model kanal AWGN memberikan nilai BER yang lebih baik dari model kanal Rayleigh. Hal ini terjadi karena pada model kanal AWGN, gangguan yang dialami sinyal adalah faktor tambahan *noise* saja, sementara pada model kanal Rayleigh ada gangguan dari efek *multipath* yang ikut merusak pulsa-pulsa sinyal ADS-B sehingga lebih banyak bit yang *error*.

Terlihat pula bahwa BER sistem tanpa algoritma enkripsi lebih baik dibanding BER sistem yang ditambahkan algoritma enkripsi yang diterapkan, yaitu Algoritma Blowfish 8 bit. Hal ini terjadi akibat adanya tambahan proses pengolahan bit-bit informasi sehingga kemungkinan terjadinya *error* pada bit-bit informasi semakin tinggi.

BAB 5
PENUTUP

5.1 Kesimpulan

Setelah melakukan simulasi sistem ADS-B dengan penambahan Algoritma Blowfish 8 Bit, kesimpulan yang diperoleh adalah sebagai berikut.

1. Algoritma Blowfish 8 Bit hasil rancangan:
   a. berhasil melakukan proses enkripsi dan dekripsi sesuai rencana.
   b. memiliki nilai *Avalanche Effect* lebih dari atau sama dengan 50% di *round* 10 dan 16.
   c. menghasilkan *cipher* dengan korelasi linier yang rendah terhadap *plaintext*, dengan rata-rata -0,004716.
   d. menghasilkan *cipher* yang membutuhkan waktu selama $4{,}175017 \times 10^{15}$ detik untuk dibongkar menggunakan metode *brute force attack* menggunakan komputer dengan spesifikasi sama dengan komputer untuk penelitian ini.
   e. memberikan tambahan waktu pengolahan infromasi di *receiver* ADS-B selama rata-rata 0,0944 detik.
2. BER sistem di kanal AWGN lebih baik daripada di kanal Rayleigh, dan BER sistem tanpa algoritma enkripsi lebih baik daripada sistem dengan algoritma enkripsi.

5.2 Saran

Dalam melakukan simulasi sistem ADS-B dan algoritma enkripsi selanjutnya, perlu diperhatikan beberapa hal sebagai berikut

1. Menggunakan *software* khusus simulasi algoritma enkripsi yang menggunakan standar bahasa C atau C++ sehingga bisa mensimulasikan algoritma enkripsi sesuai standar untuk mendapatkan hasil pengukuran yang lebih akurat dan tanpa memerlukan modifikasi algoritma enkripsi seperti yang perlu dilakukan pada MATLAB.
2. Dilakukan pengukuran langsung, misalnya menggunakan WARP, sehingga didapatkan hasil pengukuran pada keadaan nyata sebagai pembading terhadap hasil simulasi.
3. Menggunakan komputer dengan spesifikasi *clock speed* prosesor dan RAM yang lebih tinggi agar mampu melakukan simulasi dengan jumlah data yang lebih banyak.

Halaman ini sengaja dikosongkan

DAFTAR PUSTAKA

[1] Eurocontrol. *ADS-B for Dummies*

[2] International Civil Aviation Organization, 2003, *What is ADS-B?*

[3] Air Facts, *ADS-B Diagram.* <http://airfactsjournal.com/files/2013/01/ADS-B-diagram.png> diakses pada 17 Oktober 2016.

[4] Garmin, *G1000 Traffic*. <https://static.garmin.com/en/products/010-01216-00/g/g1000-traffic.jpg> diakses pada 2 Juni 2017.

[5] Hableel, Eman, Joonsang Baek, Young-Ji Byon, and Duncan S. Wong,, 2015, *How to Protect ADS-B: Confidentiality Framework for Future Air Traffic Communication*. The 2015 IEEE INFOCOM International Workshop on Mobility *Management* in the Networks of the Future World.

[6] Adsb-decode-guide.readthedocs.io, 2017, *ADS-B Decoding Guide — ADS-B Mode-S Decoding Guide documentation.* < https://adsb-decode-guide.readthedocs.io/en/latest/> diakses pada 29 Mei 2017

[7] International Civil Aviation Organization, 2003, *Manual for the Universal Access Transceiver (UAT)*.

[8] Kromodimoeljo, Sentot, Januari 2010, *Teori dan Aplikasi Kriptografi*, SPK IT Consulting. ISBN 978-602-96233-0-7.

[9] L., Srinivas B., Anish Shanbhag, Austin Solomon D'Souza, October 2014, *A Comparative Performance Analysis of DES and BLOWFISH Symmetric Algorithm*. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Special Issue 5, ISSN (Online) 2320-9801.

[10] Schneier, Bruce. *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption*, Cambridge Security Workshop Proceedings (Dec. 1993), Lecture Notes in Computer Science (LNCS) Springler verlag Vol. 809, pp. 191-204, 1993, ISBN 3- 540-58108-1.

[11] Elminaam, D. S. Abdul, H. M. Abdul Kader, M. M. Hadhoud, 2009, *Performance Evaluation of Symmetric Encryption Algorithms*. Communications of the IBIMA, Vol. 8, ISSN 1943-7765.

[12] Dr. Mitra, Abhijit, November 2009, *Lecture Notes on Mobile Communication*. pp. 96-100.

[13] Albaichi, Ashwak, Faudziah Ahmad, Ramlan Mahmod, 2013, *Security Analysis of Blowfish Algorithm*. ISBN 978-1-4673-5256-7/13.

[14] Mandal, Akash Kumar, Mrs. Archana Tiwari, 2012, *Analysis of Avalanche Effect in Plaintext of DES using Binary Codes*. International Journal of Emerging Trends and Technology in Computer Science (IJETTCS), Volume 1, Issue 3, September – October 2012, ISSN 2278-6856.

[15] Tahir, N., M. Naufal bin M. Saad, Brahim Belhaouari Samir, 2010, *Binary Pulse Position Modulation (BPPM) Bit Error Rate (BER) Analysis in Turbulent Atmospehere*. Vol. 2 No. 1, ISSN 2180-1843.

LAMPIRAN 1
LEMBAR PENGESAHAN PROPOSAL

Departemen Teknik Elektro
Fakultas Teknologi Elektro - ITS

TE 141599 TUGAS AKHIR – 4 SKS

13 FEB 2017

Nama Mahasiswa	:	Renato Simon Lawalata
Nomer Pokok	:	2213 100 032
Bidang Studi	:	Telekomunikasi Multimedia
Tugas Diberikan	:	Semester Genap 2016/2017
Dosen Pembimbing	:	Dr. Ir. Endroyono, DEA

Judul Tugas Akhir : **Peningkatan Keamanan ADS-B dengan Algoritma *Blowfish* (*ADS-B Security Improvement with Blowfish Algorithm*)**

Uraian Tugas Akhir :
Automatic Dependent Surveillance-Broadcast (ADS-B) merupakan salah satu komponen penting dalam *Air Trafic Management* (ATM) masa depan. ADS-B memungkinkan pelacakan pesawat oleh stasiun darat dengan lebih akurat sehingga potensi pesawat keluar jalur atau bahkan hilang dapat diminimalisir. Salah satu kelemahan dari teknologi ADS-B adalah keamanan kanal transmisi antara pesawat dengan stasiun darat yang lemah sehingga siapapun dengan penerima ADS-B dapat menerima sinyal yang dipancarkan pesawat, termasuk berbagai informasi dengan tingkat kerahasiaan tinggi seperti informasi militer. Untuk itu, diperlukan teknik enkripsi data yang baik untuk menyulitkan penerima ADS-B yang tidak resmi memperoleh informasi tersebut. Teknik yang digunakan adalah dengan teknik enkripsi simetris, Blowfish, dimana kekuatan enkripsi akan diukur melalui perhitungan *avalanche effect* dan koefisien korelasi antara data asli dengan data hasil enkripsi. Melalui teknik ini diharapkan aspek keamanan data tetap baik dan kecepatan dekripsi meningkat, sehingga performansi keseluruhan sistem ADS-B meningkat.

Dosen Pembimbing,

Dr. Ir. Endroyono, DEA
Nip : 196504041991021001

Mengetahui,
Ketua Program Studi S1

Dr. Dedet C. Riawan, ST. M.Eng. Ph. D.
Nip : 197111192000031001

Menyetujui,
Kepala Laboratorium Telekomunikasi Multimedia

Dr. Ir. Endroyono, DEA
Nip : 196504041991021001

Halaman ini sengaja dikosongkan

LAMPIRAN 2
LISTING PROGRAM DAN HASIL SIMULASI

1. Script MATLAB Blowfish 8 Bit

```
%PEMBANGKITAN INPUT
bitbit=input('Ingin input berapa bit ? ');
x = randi([0 1],1,bitbit);
panjang_data = bitbit;
stopper = ceil(panjang_data/8);
x2 = [x zeros(1,8*stopper-panjang_data)];
inputt = reshape(x2,8,[])';
ukuran = size(inputt);
%INISIALISASI P-ARRAY dan S-BOX
P_array = [6 08 13 5 8 1 6 2 2 4 05 4 3 5 5 3 2 04];
%dari nilai desimal pi
S_box = [4 08; 7 8; 5 7; 7 011]; %dari nilai desimal pi
%INPUT KEY
length_key = randi([1 56],1); %panjang key diatur acak
key = randi([0 2^(length_key-1)],1); %nilai desimal key
diatur acak
keybit = fliplr(de2bi(key,length_key+1));
%persiapan untuk P-array dan S-box baru / Subkey
Generation
%P_array jadi biner
P_array_biner = reshape(fliplr(de2bi(P_array))',1,[]);
%Key jadi biner
key_p =
repmat(keybit,1,ceil(length(P_array_biner)/length_key));
key_p = key_p(1:length(P_array_biner));
%P_array biner XOR Key_biner
P_array_biner_new = xor(P_array_biner,key_p);
%Persiapan sebelum komputasi
inputt2 = zeros(1,8);
ukuran2 = size(inputt2);
crypt = zeros(ukuran2);
```

```
%UPDATE P_array
for h = 1:9
for g = 1:ukuran2(1,1)
%ENCRYPT
left_bit = inputt2(g,1:4);
right_bit = inputt2(g,5:8);
%feistel_network
modulus = length(left_bit);
left_bit2 = left_bit;
right_bit2 = right_bit;
for i = 1:16
firstxor =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(i));
dummy = firstxor;
S_box_value = fliplr(de2bi(firstxor,modulus));
for j = 1:4
S(j) = S_box(j,S_box_value(j)+1);
end
Feistel_AND_1 = mod(bitand(S(1),S(2)),2^modulus-1);
Feistel_XOR_1 = bitxor(Feistel_AND_1,S(3));
Feistel_AND_2 = mod(bitand(Feistel_XOR_1,S(4)),2^modulus-
1);
Feistel_XOR_2 =
bitxor(Feistel_AND_2,bi2de(fliplr(right_bit2)));
left_bit2 = fliplr(de2bi(Feistel_XOR_2));
right_bit2 = fliplr(de2bi(dummy));
%FEISTEL NETWORK DIULANG 16 kali
end
%XOR terakhir
left_last_XOR =
bitxor(bi2de(fliplr(right_bit2)),P_array_new(18));
right_last_XOR =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(17));
%2 kelompok 4 bit menjadi 1 kelompok 8 bit
crypt(g,:) = [fliplr(de2bi(left_last_XOR,modulus)),
fliplr(de2bi(right_last_XOR,modulus))];
end
P_array_new(2*h) = bi2de(fliplr(crypt(5:8)));
P_array_new(2*h-1) = bi2de(fliplr(crypt(1:4)));
inputt2 = crypt;
end
```

```
%UPDATE S_box
S_box_new = S_box;
for f = 1:4
for g = 1:ukuran2(1,1)
%ENCRYPT
left_bit = inputt2(g,1:4);
right_bit = inputt2(g,5:8);
%feistel_network
modulus = length(left_bit);
left_bit2 = left_bit;
right_bit2 = right_bit;
for i = 1:16
firstxor =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(i));
dummy = firstxor;
S_box_value = fliplr(de2bi(firstxor,modulus));
for j = 1:4
S(j) = S_box_new(j,S_box_value(j)+1);
end
Feistel_AND_1 = mod(bitand(S(1),S(2)),2^modulus-1);
Feistel_XOR_1 = bitxor(Feistel_AND_1,S(3));
Feistel_AND_2 = mod(bitand(Feistel_XOR_1,S(4)),2^modulus-
1);
Feistel_XOR_2 =
bitxor(Feistel_AND_2,bi2de(fliplr(right_bit2)));
left_bit2 = fliplr(de2bi(Feistel_XOR_2));
right_bit2 = fliplr(de2bi(dummy));
%FEISTEL NETWORK DIULANG 16 kali
end
%XOR terakhir
left_last_XOR =
bitxor(bi2de(fliplr(right_bit2)),P_array_new(18));
right_last_XOR =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(17));
%2 kelompok 4 bit menjadi 1 kelompok 8 bit
crypt(g,:) = [fliplr(de2bi(left_last_XOR,modulus)),
fliplr(de2bi(right_last_XOR,modulus))];
end
S_box_new(f,2) = bi2de(fliplr(crypt(5:8)));
S_box_new(f,1) = bi2de(fliplr(crypt(1:4)));
inputt2 = crypt;
end
```

```
%Masuk ke komputasi Blowfish untuk plaintext
crypt = zeros(size(inputt));
for g = 1:ukuran(1,1)
%ENCRYPT
left_bit = inputt(g,1:4);
right_bit = inputt(g,5:8);
%feistel_network
modulus = length(left_bit);
left_bit2 = left_bit;
right_bit2 = right_bit;
for i = 1:16
firstxor =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(i));
dummy = firstxor;
S_box_value = fliplr(de2bi(firstxor,modulus));
for j = 1:4
S(j) = S_box_new(j,S_box_value(j)+1);
end
Feistel_AND_1 = mod(bitand(S(1),S(2)),2^modulus-1);
Feistel_XOR_1 = bitxor(Feistel_AND_1,S(3));
Feistel_AND_2 = mod(bitand(Feistel_XOR_1,S(4)),2^modulus-
1);
Feistel_XOR_2 =
bitxor(Feistel_AND_2,bi2de(fliplr(right_bit2)));
left_bit2 = fliplr(de2bi(Feistel_XOR_2));
right_bit2 = fliplr(de2bi(dummy));
%=> FEISTEL NETWORK DIULANG 16 kali
end
%XOR terakhir
left_last_XOR =
bitxor(bi2de(fliplr(right_bit2)),P_array_new(18));
right_last_XOR =
bitxor(bi2de(fliplr(left_bit2)),P_array_new(17));
%2 kelompok 4 bit menjadi 1 kelompok 8 bit
crypt(g,:) = [fliplr(de2bi(left_last_XOR,modulus)),
fliplr(de2bi(right_last_XOR,modulus))];
end
cipher = reshape(crypt,1,[]); %hasil enkripsi
%ENKRIPSI SELESAI
%-------------------------------------------
```

```
%PERSIAPAN DEKRIPSI
cipher2 = reshape(cipher,[],8);
crypt2 = zeros(size(inputt));
for g = 1:ukuran(1,1)
%DECRYPT
%Input
input2 = cipher2;
%kelompok 8 bit menjadi 2 kelompok 4 bit
left_bit_2 = input2(g,1:4);
right_bit_2 = input2(g,5:8);
modulus2 = length(left_bit);
%feistel_network
left_bit_2_2 = left_bit_2;
right_bit_2_2 = right_bit_2;
for i2 = 18:-1:3
firstxor2 =
bitxor(bi2de(fliplr(left_bit_2_2)),P_array_new(i2));
dummy2 = firstxor2;
S_box_value2 = fliplr(de2bi(firstxor2,modulus2));
for j2 = 1:4
S2(j2) = S_box_new(j2,S_box_value2(j2)+1);
end
Feistel2_AND_1 = mod(bitand(S2(1),S2(2)),2^modulus2);
Feistel2_XOR_1 = bitxor(Feistel2_AND_1,S2(3));
Feistel2_AND_1 =
mod(bitand(Feistel2_XOR_1,S2(4)),2^modulus2);
Feistel2_XOR_1 =
bitxor(Feistel2_AND_1,bi2de(fliplr(right_bit_2_2)));
left_bit_2_2 = fliplr(de2bi(Feistel2_XOR_1));
right_bit_2_2 = fliplr(de2bi(dummy2));
%FEISTEL NETWORK DIULANG 16 kali
end
%XOR terakhir
left_last_XOR_2 =
bitxor(bi2de(fliplr(right_bit_2_2)),P_array_new(1));
right_last_XOR_2 =
bitxor(bi2de(fliplr(left_bit_2_2)),P_array_new(2));
%2 kelompok 4 bit menjadi 1 kelompok 8 bit
crypt2(g,:)    =
[fliplr(de2bi(left_last_XOR_2,modulus2)),fliplr(de2bi(rig
ht_last_XOR_2,modulus2))];
end
crypt3 = reshape(crypt2',1,[]); %kembali menjadi
plaintext
```

2. Tabel Hasil Perhitungan Koefisien Korelasi

Nomor	Nilai Koefisien Korelasi
1	-0,040700
2	-0,030800
3	0,070600
4	0,001600
5	-0,035700
6	-0,061900
7	-0,124100
8	0,179000
9	0,036000
10	-0,008400
11	-0,231700
12	-0,023600
13	-0,121700
14	-0,129300
15	-0,098100
16	-0,133300
17	0,228400
18	0,327300
19	0,066700
20	-0,057600
21	0,120400
22	0,095300
23	-0,071600
24	0,187900

Nomor	Nilai Koefisien Korelasi
25	-0,076900
26	0,051800
27	0,160200
28	-0,021700
29	-0,054300
30	-0,025000
31	0,000000
32	-0,054000
33	0,000000
34	0,103200
35	-0,018500
36	-0,021100
37	-0,177800
38	-0,110300
39	-0,107400
40	-0,107200
41	0,106000
42	0,023800
43	0,002300
44	0,040700
45	-0,070200
46	-0,053000
47	-0,117500
48	-0,036000
49	0,191000

Nomor	Nilai Koefisien Korelasi
50	-0,072500
51	0,019200
52	0,035400
53	0,039900
54	0,052000
55	-0,136300
56	0,017900
57	0,096300
58	-0,024800
59	-0,024400
60	-0,326700
61	-0,143700
62	0,031100
63	0,125000
64	0,058500
65	-0,072800
66	0,115400
67	-0,076400
68	0,040400
69	-0,112800
70	0,065300
71	-0,022500
72	-0,202600
73	-0,162300
74	0,069100

Nomor	Nilai Koefisien Korelasi
75	-0,107500
76	-0,098200
77	-0,169400
78	0,118000
79	-0,001300
80	0,151500
81	0,127200
82	-0,071800
83	-0,071100
84	0,063700
85	-0,107200
86	0,016000
87	-0,130600
88	-0,143200
89	0,267400
90	-0,072600
91	0,070500
92	0,103200
93	0,034500
94	0,213800
95	0,057600
96	-0,010300
97	0,087600
98	-0,047400
99	0,106000

Nomor	Nilai Koefisien Korelasi
100	-0,018500
Rata-rata	-0,004716

3. Tabel Hasil Perhitungan Durasi

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
1	0,001879	0,008688	0,08849695	0,0972
2	0,001292	0,004390	0,081738765	0,0861
3	0,001084	0,001949	0,068247589	0,0702
4	0,000994	0,001247	0,0638146	0,0651
5	0,000946	0,003409	0,133373611	0,1368
6	0,000931	0,001595	0,08639289	0,0880
7	0,000590	0,001094	0,062159811	0,0633
8	0,001083	0,001208	0,078809876	0,0800
9	0,001821	0,001173	0,08293682	0,0841
10	0,000957	0,001819	0,073747536	0,0756
11	0,000696	0,001799	0,068300773	0,0701
12	0,000734	0,001041	0,065152614	0,0662
13	0,000636	0,001512	0,06484237	0,0664
14	0,000630	0,001588	0,064015675	0,0656
15	0,000832	0,001316	0,068503248	0,0698
16	0,001341	0,000886	0,067116715	0,0680

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
17	0,001092	0,001330	0,079346388	0,0807
18	0,001293	0,000983	0,065405008	0,0664
19	0,000699	0,001220	0,060560072	0,0618
20	0,000813	0,001304	0,128714354	0,1300
21	0,000652	0,001374	0,085856378	0,0872
22	0,000557	0,001092	0,060434108	0,0615
23	0,000876	0,000927	0,064303526	0,0652
24	0,000851	0,001349	0,104927279	0,1063
25	0,000638	0,001100	0,058436417	0,0595
26	0,000649	0,001190	0,05923792	0,0604
27	0,001030	0,001710	0,074388085	0,0761
28	0,000635	0,000996	0,059084431	0,0601
29	0,000760	0,001431	0,066697769	0,0681
30	0,000593	0,001215	0,063815067	0,0650
31	0,000621	0,001034	0,062797094	0,0638
32	0,000642	0,000971	0,057940494	0,0589
33	0,000574	0,001099	0,06354821	0,0646
34	0,000765	0,001405	0,063062084	0,0645
35	0,000736	0,000899	0,059153011	0,0601
36	0,001219	0,000929	0,059708651	0,0606
37	0,000618	0,001036	0,060577334	0,0616

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
38	0,000898	0,002301	0,090092957	0,0924
39	0,000825	0,001070	0,11575829	0,1168
40	0,000739	0,001194	0,11076173	0,1120
41	0,000856	0,001025	0,133459919	0,1345
42	0,000834	0,001015	0,105054176	0,1061
43	0,000608	0,001682	0,083477997	0,0852
44	0,000540	0,001102	0,065167077	0,0663
45	0,000516	0,001000	0,060809667	0,0618
46	0,001165	0,001453	0,060457901	0,0619
47	0,000827	0,001028	0,064871295	0,0659
48	0,000640	0,000915	0,061593441	0,0625
49	0,000634	0,001108	0,066674909	0,0678
50	0,000955	0,000955	0,085398244	0,0864
51	0,000887	0,001337	0,075747093	0,0771
52	0,000948	0,002310	0,102968777	0,1053
53	0,001119	0,001426	0,111789034	0,1132
54	0,000618	0,001113	0,087974901	0,0891
55	0,000703	0,001289	0,066901643	0,0682
56	0,000809	0,001109	0,071601955	0,0727
57	0,001101	0,000947	0,063179183	0,0641
58	0,000585	0,000965	0,064877827	0,0658

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
59	0,000542	0,002170	0,081471909	0,0836
60	0,000718	0,006024	0,109079882	0,1151
61	0,000555	0,001405	0,068765439	0,0702
62	0,000534	0,001563	0,089146829	0,0907
63	0,000917	0,001089	0,074246726	0,0753
64	0,000662	0,002079	0,091573263	0,0937
65	0,000714	0,001324	0,078835069	0,0802
66	0,000570	0,001189	0,083855422	0,0850
67	0,000727	0,001539	0,083598362	0,0851
68	0,000457	0,001421	0,083228869	0,0846
69	0,000476	0,001261	0,092865091	0,0941
70	0,000428	0,001273	0,075274496	0,0765
71	0,000434	0,003297	0,066219573	0,0695
72	0,000472	0,001106	0,070757065	0,0719
73	0,000720	0,001123	0,066634787	0,0678
74	0,000421	0,001164	0,076294335	0,0775
75	0,000863	0,002929	0,075200317	0,0781
76	0,000555	0,000972	0,066366064	0,0673
77	0,000540	0,001263	0,076309264	0,0776
78	0,000458	0,001209	0,084486173	0,0857
79	0,000674	0,001524	0,072528954	0,0741

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
80	0,001432	0,002041	0,092013203	0,0941
81	0,000627	0,002584	0,077074843	0,0797
82	0,000483	0,001320	0,078434318	0,0798
83	0,000401	0,003786	0,072483234	0,0763
84	0,000453	0,001190	0,083785442	0,0850
85	0,000422	0,000964	0,071930393	0,0729
86	0,000410	0,001256	0,099383944	0,1006
87	0,000475	0,001931	0,08005925	0,0820
88	0,000555	0,001345	0,071270717	0,0726
89	0,000795	0,001054	0,081656656	0,0827
90	0,000509	0,002042	0,077823161	0,0799
91	0,000430	0,001058	0,072077818	0,0731
92	0,000429	0,001458	0,06808197	0,0695
93	0,000756	0,001059	0,098621164	0,0997
94	0,000941	0,001124	0,077542775	0,0787
95	0,001144	0,001145	0,080285051	0,0814
96	0,000697	0,001153	0,067313125	0,0685
97	0,000528	0,001124	0,070907755	0,0720
98	0,000491	0,000895	0,072263031	0,0732
99	0,000717	0,001002	0,086410152	0,0874
100	0,000525	0,001228	0,08500729	0,0862

Nomor	Durasi Pengolahan Informasi di *Receiver* Sebelum Penambahan Blowfish (detik)	Durasi Demodulasi PPM (detik)	Durasi Dekripsi (detik)	Total Durasi Pengolahan Informasi di *Receiver* Sesudah Penambahan Blowfish (detik)
Rata-rata	0,000752	0,001533	0,077554	0,079088

4. Tabel Hasil Perhitungan *Avalanche Effect*

	Jumlah Bit Berubah Pada Percobaan ke-				
Round	1	2	3	4	5
1	1	1	1	2	2
2	2	3	3	4	3
3	2	3	3	3	2
4	3	3	3	3	3
5	3	3	3	2	2
6	4	3	3	4	5
7	2	3	3	3	2
8	1	1	1	1	1
9	3	3	3	2	2
10	5	4	4	3	4
11	4	3	3	3	4
12	3	3	3	3	3
13	2	2	2	3	3
14	2	3	3	4	3
15	2	3	3	3	2
16	4	4	4	4	4

	Jumlah Bit Berubah Pada Percobaan ke-				
Round	6	7	8	9	10
1	1	2	1	1	2
2	3	3	3	2	4
3	3	2	3	2	3
4	3	3	3	3	3
5	3	2	3	3	2
6	3	5	3	4	4
7	3	2	3	2	3
8	1	1	1	1	1
9	3	2	3	3	2
10	4	4	4	5	3
11	3	4	3	4	3
12	3	3	3	3	3
13	2	3	2	2	3
14	3	3	3	2	4
15	3	2	3	2	3
16	4	4	4	4	4

	Jumlah Bit Berubah Pada Percobaan ke-				
Round	11	12	13	14	15
1	1	2	1	1	1
2	2	4	2	3	2
3	2	3	2	3	2
4	3	3	3	3	3

5	3	2	3	3	3
6	4	4	4	3	4
7	2	3	2	3	2
8	1	1	1	1	1
9	3	2	3	3	3
10	5	3	5	4	5
11	4	3	4	3	4
12	3	3	3	3	3
13	2	3	2	2	2
14	2	4	2	3	2
15	2	3	2	3	2
16	4	4	4	4	4

	Jumlah Bit Berubah Pada Percobaan ke-				
Round	16	17	18	19	20
1	2	1	1	1	1
2	4	2	3	2	3
3	3	2	3	2	3
4	3	3	3	3	3
5	2	3	3	3	3
6	4	4	3	4	3
7	3	2	3	2	3
8	1	1	1	1	1
9	2	3	3	3	3
10	3	5	4	5	4
11	3	4	3	4	3

	Jumlah Bit Berubah Pada Percobaan ke-				
Round	16	17	18	19	20
12	3	3	3	3	3
13	3	2	2	2	2
14	4	2	3	2	3
15	3	2	3	2	3
16	4	4	4	4	4

BIODATA PENULIS

Penulis yang bernama lengkap Renato Simon Lawalata lahir pada 19 Oktober 1995. Penulis merupakan anak dari pasangan Bapak Floyd Wilbert Ray Lawalata dan Ibu Eti Mandiangan. Penulis lahir di Jakarta, tetapi tumbuh di Tangerang. Pendidikan formal penulis dimulai dari SD Strada Santa Maria Tangerang yang diselesaikan pada tahun 2007, dilanjutkan ke SMPN 1 Tangerang yang diselesaikan pada tahun 2010, kemudian ke SMAN 2 Tangerang yang diselesaikan pada tahun 2013. Penulis melanjutkan Pendidikan Strata 1 dengan mendaftar ke Departemen Teknik Elektro, Fakultas Teknologi Elektro, Insitut Teknologi Sepuluh Nopember dan masuk pada tahun 2013, yang pada waktu itu masih bernama Jurusan Teknik Elektro, Fakultas Teknologi Industri, Institut Teknologi Sepuluh Nopember, dimana penulis memilih masuk ke bidang studi Telekomunikasi Multimedia. Selain mengikuti kegiatan akademik, penulis pernah tergabung dalam Dewan Perwakilan Angkatan HIMATEKTRO ITS di semester 3-6 perkuliahan dan menjadi asisten kegiatan Praktikum Dasar Sistem Telekomunikasi di semester 5 & 7 dan Praktikum Komunikasi Data dan Pengolahan Sinyal Digital di semester 6 & 8. Penulis dapat dihubungi melalui email di renato19id@gmail.com.

Halaman ini sengaja dikosongkan